ICS 33.040
M 10

YD

中华人民共和国通信行业标准

YD/T 1858-2009

2GHz TD-SCDMA/WCDMA 数字蜂窝移动通信网 通用认证架构（第二阶段）

Digital Cellular Mobile Telecommunication Network Generic Authentication Architecture for 2GHz TD-SCDMA/WCDMA（Phase 2）

2009-06-15 发布 2009-09-01 实施

中华人民共和国工业和信息化部 发布

目　次

前　言……III
1　范围……1
2　规范性引用文件……1
3　定义和缩略语……3
4　通用认证架构的系统性描述（终端分离情况下的通用认证解决方案详见附录 K）……6
4.1　总体介绍……6
4.2　GAA 介绍……7
4.3　发放认证凭证……8
4.4　GAA 结构模块……8
4.5　使用 GAA 的应用指南……10
4.6　GBA 的使用……12
5　GBA 过程……13
5.1　GBA 架构……13
5.2　UICC 增强型 GBA（GBA_U）……27
5.3　终端分离情况下的增强通用认证框架……33
6　用户证书的支持……33
7　UE 采用 HTTPS 接入 NAF……42
7.1　安全构架概述……42
7.2　认证机制……42
7.3　认证代理的使用……48
8　通用认证框架 Push 功能……51
8.1　概述……51
8.2　GBA Push 架构描述及基本原理……51
8.3　GBA Push 需求……52
8.4　GBA Push 功能……54
附录 A（规范性附录）　密钥衍生函数 KDF 的规范……56
附录 B（资料性附录）　GBA 中，用户选择 UICC 应用的对话框实例……58
附录 C（规范性附录）　保护参考点 Zn/Zn′的 TLS 描述文件……59
附录 D（资料性附录）　TLS 证书的处理……60
附录 E（规范性附录）　GBA_U UICC-ME 接口……61
附录 F（资料性附录）　密钥对存储……63
附录 G（资料性附录）　通过认证代理和 HTTPS 接入到应用服务器的技术方案……69
附录 H（资料性附录）　UE 和应用服务器间基于证书的互认证向导……70

标准分享网 www.bzfxw.com 免费下载

附录 I（规范性附录） 2G GBA……71
附录 J（资料性附录） 具备 GBA 功能的漫游用户访问漫游网络的 GAA 应用……83
附录 K（资料性附录） 终端分离情况下的通用认证解决方案……84

前　言

本标准是2GHz TD-SCDMA/WCDMA数字蜂窝移动通信网通用认证架构系列标准之一，该系列标准结构如下：

a）YD/T 1857-2009　2GHz TD-SCDMA/WCDMA数字蜂窝移动通信网通用认证架构（第一阶段）

b）YD/T 1858-2009　2GHz TD-SCDMA/WCDMA数字蜂窝移动通信网通用认证架构（第二阶段）

本标准与《2GHz TD-SCDMA/WCDMA数字蜂窝移动通信网通用认证架构（第一阶段）》相比较，增加了通用认证架构push功能章节（第8章），2G GBA功能（附录I），具备GBA功能的漫游用户访问漫游网络GAA应用（附录J），终端分离情况下的通用认证架构需求和解决方案（5.3节和附录K）。

本标准主要参考3GPP TR 33.919 V 7.2.0、TS 33.220 V 7.7.0、TS33.221 V 6.3.0，TS33.222 V 7.2.0以及TS33.223 V0.3.0。

— 第4章与3GPP TR 33.919 V 7.2.0的第4～7章在技术内容上保持一致：

- 其中第4.1节对应于3GPP TR 33.919 V 7.2.0的概述部分；
- 其中第4.2节对应于3GPP TR 33.919 V 7.2.0的第4章部分；
- 其中第4.3节对应于3GPP TR 33.919 V 7.2.0的第5章部分；
- 其中第4.4节对应于3GPP TR 33.919 V 7.2.0的第6章部分；
- 其中第4.5节对应于3GPP TR 33.919 V 7.2.0的第7章部分。

— 第5章与3GPP TS 33.220 V 7.7.0的第4～5章在技术内容上保持一致：

- 其中第5.1节对应于3GPP TS 33.220 V 7.7.0的第4章部分；
- 其中第5.2节对应于3GPP TS 33.220 V 7.7.0的第5章部分。

— 第6章与3GPP TS 33.221 V 6.3.0的第4章在技术内容上保持一致：

— 第7章与3GPP TS 33.222 V 7.2.0的第4～6章在技术内容上保持一致：

- 其中第7.1节对应于3GPP TS 33.222 V 7.2.0的第4章部分；
- 其中第7.2节对应于3GPP TS 33.222 V 7.2.0的第5章部分；
- 其中第7.3节对应于3GPP TS 33.222 V 7.2.0的第6章部分。

— 第9章与3GPP TS 33.223 V 0.3.0的部分在技术内容上保持一致。

— 附录A与3GPP TS 33.220V 7.7.0的Annex B在技术内容上保持一致。

— 附录B与3GPP TS 33.220V 7.7.0的Annex D在技术内容上保持一致。

— 附录C与3GPP TS 33.220V 7.7.0的Annex E在技术内容上保持一致。

— 附录D与3GPP TS 33.220V 7.7.0的Annex F在技术内容上保持一致。

— 附录E与3GPP TS 33.220V 7.7.0的Annex G在技术内容上保持一致。

— 附录F与3GPP TS 33.221V 6.3.0的Annex A在技术内容上保持一致。

— 附录G与3GPP TS 33.222V 7.2.0的Annex A在技术内容上保持一致。

— 附录H与3GPP TS 33.222V 7.2.0的Annex B在技术内容上保持一致。

— 附录I与3GPP TS 33.220V 7.7.0的Annex I在技术内容上保持一致。

标准分享网 www.bzfxw.com 免费下载

本标准的附录A、附录C、附录E、附录I为规范性附录，附录B、附录D、附录F、附录G、附录H、附录J、附录K为资料性附录。

本标准由中国通信标准化协会提出并归口。

本标准起草单位：华为技术有限公司、诺基亚通信有限公司、中国移动通信集团公司、上海贝尔阿尔卡特股份有限公司、青岛朗讯科技通讯设备有限公司、南京爱立信熊猫通信有限公司、工业和信息化部电信研究院

本标准主要起草人：许怡娴、杨艳梅、黄迎新、张大江、刘　斐、朱红儒、袁兵兵、胡志远、南明凯

2GHz TD-SCDMA/WCDMA 数字蜂窝移动通信网 通用认证架构（第二阶段）

1 范围

本标准规定了2GHz TD-SCDMA/WCDMA数字蜂窝移动通信网通用认证框架的架构模型，协议体系，通用认证框架的认证与密钥协商的流程，通用认证框架的使用，漫游应用以及扩展的push业务应用。

本标准适用于用户访问TD-SCDMA/WCDMA网络中多种应用业务。

2 规范性引用文件

下列文件中的条款通过本标准的引用而成为本标准的条款。凡是注日期的引用文件，其随后所有的修改单（不包括勘误的内容）或修订版均不适用于本标准。然而，鼓励根据本标准达成协议的各方研究是否可使用这些文件的最新版本。凡是不注日期的引用文件，其最新版本适用于本标准。

3GPP TS 33.102：第三代伙伴计划；技术规范组，服务与系统方面；3G安全；安全架构

IETF RFC 2818：TLS上的HTTP

3GPP TS 29.109：第三代伙伴计划；技术规范组，核心网；通用认证架构（GAA）；基于Diameter协议的Zh和Zn接口；协议详述

3GPP TS 24.109：第三代伙伴计划；技术规范组，核心网；Bootstrapping接口（Ub）和网络应用功能接口（Ua）；协议详述

3GPP TS 29.198 03：第三代伙伴计划；技术规范组，核心网；开放服务接入（OSA）；应用编程接口（API）；第三部分：框架

3GPP TS 29.199-01：第三代伙伴计划；技术规范组，核心网；开放服务接入（OSA）；Parlay X 网络服务；第一部分：Common

3GPP TS 31.102：第三代伙伴计划；技术规范组，终端；USIM应用的特征

OMA：Provisioning内容版本1.1，版本2003年8月13日　开放移动联盟

IETF RFC 3546（2003）：运输层安全（TLS）扩展

3GPP TS 31.103：第三代伙伴计划；技术规范组，终端；IP多媒体服务身份模块（ISIM）应用的特征

3GPP TS 23.003：第三代伙伴计划；技术规范组，核心网；Numbering,addressing and identification

3GPP TS 33.210：第三代伙伴计划；技术规范组，服务与系统方面；3G安全；网络域安全；IP网络层安全

IETF RFC 3588(2003)：Diameter协议

3GPP TS 31.101：第三代伙伴计划；技术规范组，终端；UICC终端接口；物理和逻辑特性

IETF RFC 3280（2002）：因特网X.509公钥基础设施证书和证书撤销列表(CRL)描述

3GPP TS 33.310：第三代伙伴计划；技术规范组，服务与系统方面；网络域安全(NDS)；认证框架(AF)

FIPS PUB 180-2(2002)：安全Hash标准

IETF RFC 2104(1997)：HMAC：消息认证的hash密钥

标准分享网 www.bzfxw.com 免费下载

ISO/IEC 10118-3:2004：信息技术—安全技术—Hash函数—第三部分：专用的hash函数

IETF RFC 3629(2003)：UTF-8，ISO 10646的转换格式

PKCS#10：IETF RFC 2510　证书请求语法标准

IETF RFC 2510：因特网X.509公钥基础设施证书管理协议

IETF RFC 2511：因特网X.509证书请求信息格式

IETF RFC 2527：因特网X.509公钥基础设施公钥政策和证书实践框架

OMA：WAP证书和CRL描述

OMA：无线身份模块；安全

OMA：无线应用描述；公钥基础设施定义

ITU T Recommendation X.509(1997)| ISO/IEC 9594-8:1997：信息技术—开放系统互联—目录：认证框架

OMA：ECMAScript移动文件的密码对象

欧洲国会和理事会关于电子信号的通信架构：Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures

IETF RFC 3039：因特网X.509公钥基础设施合格证书描述

ETSI TS 101 862：合格证书描述

IETF RFC 2797：CMS上的证书管理信息

3GPP TS 23.002：网络架构

3GPP TS 22.250：IP多媒体子系统（IMS）组管理；阶段1

3GPP TS 33.141：第三代伙伴计划；技术规范组，服务与系统方面；Presence服务；安全

IETF RFC 2246(1999)：TLS协议版本1

IETF RFC 3268(2002)：运输层安全（TLS）高级加密标准（AES）密码组

IETF RFC 3310(2002)：使用AKA算法的超文本传输协议密码组

IETF RFC 2616(1999）：超文本传输协议（HTTP）– HTTP/1.1

OMAWAP-219-TLS,4.11.2001:

http://www.openmobilealliance.org/tech/affiliates/wap/wap-219-tls-20010411-a.pdf

OMAWAP-211-WAPCert,22.5.2001:

http://www.openmobilealliance.org/tech/affiliates/wap/wap-211-wapcert-20010522-a.pdf

W3C：网络服务描述语言（WSDL）版本2，部分0：初级

http: //www.w3.org/TR/2005/WD-wsdl20-primer-20050803/

IETF RFC4279(2005）：传输层安全（TLS）的预共享密码组

3GPP TS 33.246：第三代伙伴计划；技术规范组，服务与系统方面；3G安全，多媒体广播/多波服务的安全

3GPP TR 33.905：第三代伙伴计划；技术规范组，服务与系统方面；可信开放平台的建议

3GPP TR 33.920：第三代伙伴计划；技术规范组，服务与系统方面；基于GBA架构的SIM卡；早期应用特性

3GPP TS 33.110：第三代伙伴计划；技术规范组，服务与系统方面；UICC和终端的密钥建立

3GPP TR33.980：第三代伙伴计划；技术规范组，服务与系统方面；自由联盟和3GPP安全互通；自由联盟身份联合框架（ID-FF），身份网络服务框架（ID-WSF）和GAA

3 缩略语和定义

3.1 缩略语

下列缩略语适用于本标准。

AK	Anonymity Key	匿名密钥
AKA	Authentication and Key Agreement	认证和密钥协商
AP	Authentication Proxy	认证代理
AS	Application Server	应用服务器
B-TID	Bootstrapping Transaction Identifier	自举事务标识
BSF	Bootstrapping Server Function	自举服务功能
blob	Binary Large Object	二进制大型对象
CA	Certificate Authority	认证中心
CMMC	Certificate Management Messages over CMS	CMS证书管理消息
CMP	Certificate Management Protocols	证书管理协议
CMS	Cryptographic Message Syntax	证书管理语法
FQDN	Fully Qualified Domain Name	完整域名
GAA	Generic Authentication Architecture	通用认证架构
GBA	Generic Bootstrapping Architecture	通用自举架构
GBA_ME	ME-based GBA	基于移动设备的GBA
GBA_U	GBA with UICC-based enhancements	基于UICC增强的GBA
GUSS	GBA User Security Setting	GBA用户安全设置
HTTP	Hypertext Transfer Protocol	超文本传输协议
HTTPS	HTTP over TLS	基于TLS的HTTP
HSS	Home Subscriber System	归属用户系统
IK	Integrity Key	完整性密钥
IMPI	IP Multimedia Private Identity	IP 多媒体私有标识
IMPU	IP Multimedia Public Identity	IP 多媒体公开标识
KDF	Key Derivation Function	密钥衍生函数
Ks_int_NAF	Derived key in GBA_U which remains on UICC	在GBA_U中保存在UICC中的密钥
Ks_ext_NAF	Derived key in GBA_U	在GBA_U中的密钥
ME	Mobile Equipment	移动设备
MNO	Mobile Network Operator	移动网络运营商
NAF	Network Application Function	网络应用功能
NE	Network Element	网络单元

标准分享网 www.bzfxw.com 免费下载

PKCS	Public-Key Cryptography Standards	公钥加密标准
PKI	Public Key Infrastructure	公钥基础结构
SSC	Support for Subscriber Certificates	用户认证支持
SP	Service Provider	服务提供商
TLS	Transport Layer Security	传输层安全协议
UE	User Equipment	用户设备
USS	User Security Setting	用户安全设置
UID	User Identifier	用户标识

3.2 定义

下列定义适用于本标准。

3.2.1

用户证书（Subscriber certificate）

移动网络运营商根据用户的签阅情况给用户颁发的证书。该证书包含用户的公开密钥和可能的其他信息，比如用户某种形式的身份。

3.2.2

应用

本文档中所提到的应用，都应理解为由MNO或者第三方提供给移动用户的服务，它经常指的是一类服务，而不是安装在应用服务器上的应用实例。

3.2.3

自举（Bootstrapping）服务功能

BSF是MNO控制下的一个网络元素。BSF，HSS和UE共同参与GBA，在GBA过程中，通过执行自举过程，在网络与UE之间建立一个共享的密钥。这个共享密钥可以用在NAF和UE之间，比如说，为了认证目的。

3.2.4

自举（Bootstrapping）使用过程

在Ua参考点上应用建立安全关联的过程。

3.2.5

CA证书

一个证书机构用它的私有密钥签署它分发的所有证书。相应的CA公钥包含在证书中，称CA证书。

3.2.6

GBA功能

ME上的一个功能，它能够与BSF一起执行自举过程，并在Ua接口上提供安全关联来执行自举使用过程。当一个Ua应用想去利用自举安全关联的时候，这个Ua应用就会调用GBA功能。

2G GBA功能详见附录I。

3.2.7

基于ME的GBA

在GBA_ME中，所有的GBA相关功能都在ME当中执行。UICC不支持GBA。在本文档中如果没有限定GBA，那么就指的是基于ME的GBA。

3.2.8

基于UICC的GBA

基于UICC增强的GBA。在GBA_U中，GBA相关功能分布在ME和UICC上。

3.2.9

网络应用功能（NAF）

NAF是一个网络元素。NAF和UE之间可以应用GBA达到认证的目的，并且可以应用GBA来保护UE和NAF之间的安全通信。

3.2.10

自举（Bootstrapping）事务标识

该标识是用来在Ua、Ub和Zn参考点上绑定用户身份和密钥资料的。

3.2.11

GBA用户安全设置（GUSS）

GUSS包含BSF中相关信息元素和所有应用相关的USSs。

3.2.12

NAF组

允许分配不同的USS到代表同一种应用的NAFs的一个NAF组。这种分组在各个归属网络分别执行。比如说：一个NAF，与不同归属网络的BSFs相联系，但是这个NAF在每一个归属网络中属于不同的组。

3.2.13

Ua应用

在ME上和NAF一起去执行自举应用过程的一种应用。

3.2.14

用户安全设置（USS）

一个USS是一种应用和用户相关参数的集合，在这个用户参数集合里面定义了2个部分，一个是认证部分，这个认证部分包括用户为某个应用（比如说IMPI、IMPU等）所需的身份列表；另外一个是授权部分，这个授权部分包括一些允许标志（一些可以接入服务的标志，需要证书的类型）。有时候也称作应用相关用户安全设置。USS作为GUSS的一部分从HSS传送到BSF，如果NAF进行请求，它也可以从BSF发送到NAF。

3.2.15

HTTPS

对于本文档HTTPS指使用TLS来加强HTTP安全的广义概念。在其他背景中，如IETF、HTTPS被用来表示HTTP/TLS传输中的保留端口（443）。

3.2.16

反向代理

反向代理是一个网络服务系统，它能提供来源于其他网络服务器（AS）的页面，并且使得这些页面看起来是来源于反向代理本身。

标准分享网 www.bzfxw.com 免费下载

3.2.17

会话管理机制

使用HTTP协议时生成有状态会话的机制。

3.2.18

AUTN（*）

在GBA中，GBA_ME基于AUTN的值检查认证向量是否来自授权网络，GBA_U基于AUTN*的值对网络进行认证，如33.220所述。AUTN（*）用来指代AUTN和AUTN*。

3.2.19

GBA-PUSH-INFO

GBA-PUSH-INFO包括和GBA push密钥衍生相关的数据，即AUTN（*），RAND，NAF_ID，B-TID。

编者注：GBA-PUSH-INFO内容列表是否完整需要进一步研究。

3.3 符号

下列符号适用于本标准。

‖ 级联

⊕ 异或

3.4 约定

在本标准中，所有的数据变量以左边重要子串右边次要子串的形式呈现。一个子链可能是一个比特，字节或是其他任意长度的比特串。变量被拆分成一定数量子串，在子串中重要的子串被标识为0，次要子串标识为1，以此类推到最不重要的子串等。

4 通用认证架构的系统性描述（终端分离情况下的通用认证解决方案详见附录 K）

终端分离情况下的通用认证解决方案详见附录K。

4.1 总体介绍

本章介绍GAA的内容并对本章的编写作出解释。

很多应用都需要在进一步的通信前，在用户端（例如UE）和应用服务器之间进行双向认证。该类例子包括（但不局限于）客户端和presence服务器（可能通过认证代理）间的通信，客户端申请数字证书时与PKI入口的通信，与移动广播/多媒体服务（MBMS）内容服务器的通信，如BM-SC等等。

由于许多应用都需要同级别的认证机制，因此有必要定义一种通用认证架构（GAA）。GAA描述了一种通用认证架构，以优先能够应用于现在和将来的任何业务。

第4章可作为图1所示的通用认证架构的结构部分。在3GPP R6中，GBA，HTTPS和认证代理（AP）和证书都是GAA的基本构成单元，并在其他章节中定义。如何将这些单元组合在通用认证架构（GAA）中是本章节所阐述的内容。以后，很多内容都会加进规范满足各种应用场景。

本章节旨在概述移动应用所依赖的服务器与客户端（即用户终端）之间不同的认证机制。另外，本标准针对GAA（通用认证架构）的使用、在给定情况下和给定应用时的认证机制的选择2个方面给出了指导原则。

最后，本章节对涉及到同等级别的认证的不同的GAA规范进行了结构分析。本章节澄清技术规范和技术报告的逻辑结构，描述规范的内容并解释这些3GPP规范的内部联系以及他们与本部分的联系。

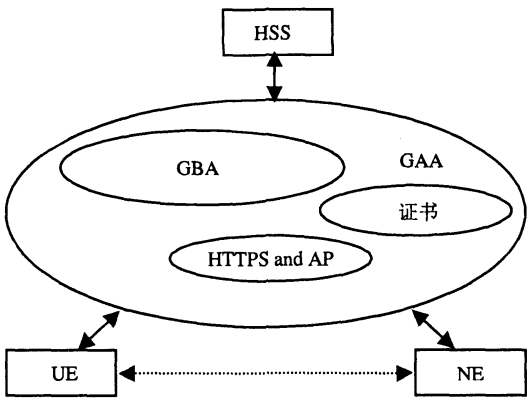


图1 GAA 的示意图

GAA的核心包括GBA。GBA的核心规范包括3GPP TS33.220，3GPP TS24.109，3GPP TS29.109。图2给出了GAA接口上使用的协议以及不同的GAA规范之间的关系。如果制定出新的GAA规范时，新的规范也会加入到图2中。-同样，将来也有可能会出现新的Ua接口，这些运行在新Ua接口上的协议，也将会添加到图2中。

TS 33.220 GBA			
TS 24.109		TS 29.109	
Ub	Ua	Zn/Zn′	Zh
HTTP Digest AKA RFC 3310	Eg.HTTP Digest RFC 2617	WSDL/SOAP based Weg Service[10]	IMS Cx Diameter message definitions TS 29.229
HTTP RFC 2616			Diameter Base Protocol RFC3588
TCP			SCTP
IP			

图2 GBA 核心规范与 GBA 接口上使用的协议间的关系

GBA会应用在很多TS和TR上来满足特定应用，如HTTPS，用户证书。

4.2 GAA 介绍

4.2.1 GAA 简介

在系统中通常有两种认证机制。一种基于通信实体间的共享秘密，另一种基于密钥对（公有或私有）。如图3所示，这两个机制在GAA中针对移动业务都是优先选项。

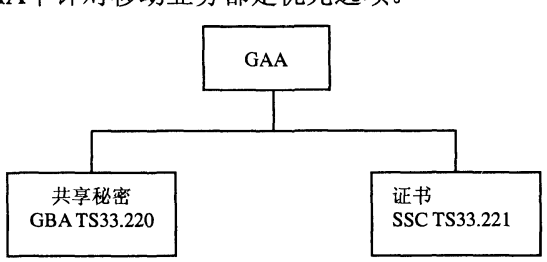


图3 GAA 示意介绍

4.2.2 基于共享秘密的认证

基于通信实体间预共享秘密机制的有若干个认证协议，常有的包括HTTP摘要，预共享密钥TLS，具有预共享秘密和优先使用用户名一密码机制的IKE协议。

这类认证机制的主要问题在于如何在该预共享秘密上保持一致。4.3.2节和第5章描述了如何在移动的上下文环境中使用基于AKA的机制为通信实体提供预共享秘密。

有关认证代理技术可参见附录G。

标准分享网 www.bzfxw.com 免费下载

4.2.3 基于密钥对（公有和私有）和证书的认证

关于认证证书和互认证内容参见附录H。

除了使用共享秘密认证外，另外一种方法基于非对称密码进行认证。该认证方法假设需要认证的实体（通信单方或者双方）拥有一个密钥对（公有和私有）以及相应的数字证书。后者验证该密钥对并绑定到其合法拥有者。众所周知的基于密钥对（公有和私有）的协议包括PGP协议、TLS上的HTTP（RFC 2818）（后者常用其协议名称HTTPS称呼）。

这类认证方法的主要缺点在于需要PKI，非对称的密钥操作与对称的密钥操作相比，经常需要更多的计算量。4.3.3节和第6章描述了一个移动运营商如何能够给其用户颁发数字证书（因而提供基本PKI）。

4.3 发放认证凭证

4.3.1 示意图

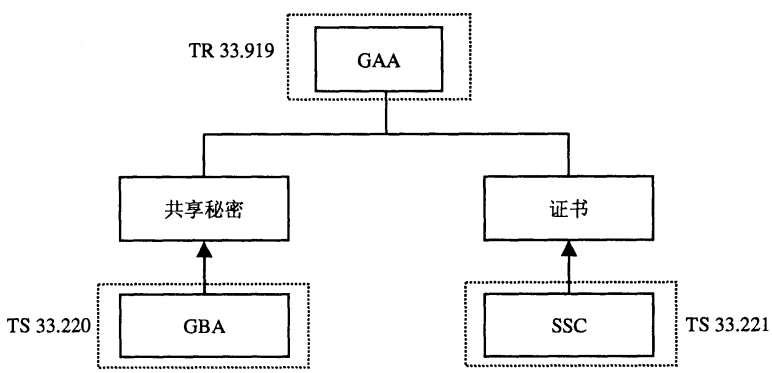


图4 发放认证凭证机制的示意图

注：用于发放认证凭证的其他机制可能存在，但超出了本部分的范围。

图4显示了TR33.919（对应于本章）与TS 33.220（对应于第5章）和TS 33.221（对应于第6章）之间的关系。一方面，第5章中所描述的基于共享秘密和GBA的认证方式指定了一种向通信双方提供共享秘密的认证机制。另一方面，第6章中所描述的基于（公、私）密钥对、数字证书和SSC的认证方式指定了如何向移动签约用户发放证书。

4.3.2 GBA：发放共享秘密机制

第5章指定了基于3GPP AKA的一个独立应用程序机制。该独立应用程序能向客户和应用程序服务器提供一个公共的共享秘密。随后，该共享秘密能用于认证客户和应用程序服务器之间的通信。

4.3.3 SSC：发放用户证书机制

第6章指定了向移动用户发放数字证书的机制。

一旦移动用户拥有一（公、私）密钥对和一数字证书，他/她就能用该证书和相应的密钥对来处理数字签名（如移动电子商务应用）和认证服务器（如TLS）。

4.4 GAA 结构模块

4.4.1 GAA 结构

本章给出了不同GAA和GBA相关文档的内容概述，并描述了它们之间如何紧密组合。

4.4.2 GAA

GAA描述了通用认证框架的体系结构。

4.4.3 GBA

如4.3.2节所述，GBA为UE和服务器建立一共享秘密而提供了一个基于3GPP AKA的通用机制。

AKA是移动网络所用的一个非常有用的机制。GBA重用AKA机制来建立应用安全。GBA引入了一个新的网元BSF。该BSF与HSS之间有一个接口。UE和HSS通过BSF来运行AKA。根据运行AKA获得的结果（CK、IK），在BSF和UE之间产生一个会话密钥。一个应用服务器（第5章中称NAF）能从BSF获得该会话密钥和签约用户档案（Profile）。通过这种方式，NAF和UE就能拥有一个共享密钥，该共享密钥能为随后的应用提供安全保护，特别是在应用会话开始时认证UE和NAF（也可能提供完整性保护和/或机密性保护，尽管完整性保护和机密性保护也许超出了GAA的范围）。UE和BSF之间的通信、NAF和BSF之间的通信、BSF和HSS之间的通信独立于应用，并在第5章有描述。

如果只有SIM卡或者UICC上SIM存在，并且允许2G GBA时，BSF和UE使用2G AKA和TLS协议进行相互认证。

以下观点导致了新网元BSF的引入：

将从HSS获取AV的所有不同类型的网元总数保持最小数目

不同应用的一个通用机制避免了各种机制之间的差异性，而且能以一致的方式阐述安全问题。

4.4.4 SSC

如果一个客户想利用非对称加密技术，他需要一个由认证中心（CA）生成的数字证书。这样的一个数字证书是将一个公开密钥和其合法拥有者的身份信息绑定在一起，并用来证明该公开密钥的合法性。如果一个移动用户想拥有和使用密钥对（公、私密钥对），该密钥对和证书应预载或该移动用户必须有方法生成或获取一个密钥对并自动获得其相应的数字证书。如4.3.3节所述，SSC为一个移动用户指定了一个自动发布数字证书的机制。

为自动获得一个数字证书，UE必须发送适当的证书请求给他归属运营商的PKI入口，该PKI入口必须认证该证书请求。事实上，证书注册过程即发放一个证书给用户和在UE和PKI入口之间的相应通信会话就是一个移动应用实例。对于很多移动应用，通信实体之间需要认证。在该情况下，UE和PKI入口之间需要进行认证（后者相当于一个应用服务器）。对于很多其他应用，认证有两个选项：基于预共享秘密、基于非对称密码算法和证书。后者只是一个选项，是指当从PKI入口获得一个新证书时而另一个有效的证书已经加载在UE里。前一个方法在PKI入口和UE之间需要一个共享秘密。如果该共享秘密不是提前预置的，则GBA能用于获得这样一个共享秘密。

如图5所示，SSC（第6章）中所述的发放一个证书给移动用户的处理过程的结果是在UE里加载一个证书及其相应的密钥对（公、私密钥对）。这由绿色的向上的箭头所示。

一旦获得证书，该证书（和相应的公私密钥对一起）能用于认证UE。这由连接证书到下面应用（图5中的HTTS和SSC）的黑色虚线所示。该公私密钥对和相应的数字证书也能用于完整性保护（或极少用于机密性保护），但这些都不是GAA的范围。

4.4.5 使用 HTTPS 访问 NAF

HTTPS（或HTTP/TLS）能用于许多业务来保护在UE和应用服务器之间（第5章、第7章所述的Ua接口）的应用会话。第7章详细描述了当HTTPS用于UE和应用服务器之间的可能认证选项。任何已有或将来基于HTTPS或预共享TLS的应用的认证和一个安全HTTPS会话的建立都能参考第7章。

4.4.5.1 有认证代理的 HTTPS

第7章描述了在UE和AS之间使用认证代理AP时的一种机制。

标准分享网 www.bzfxw.com 免费下载

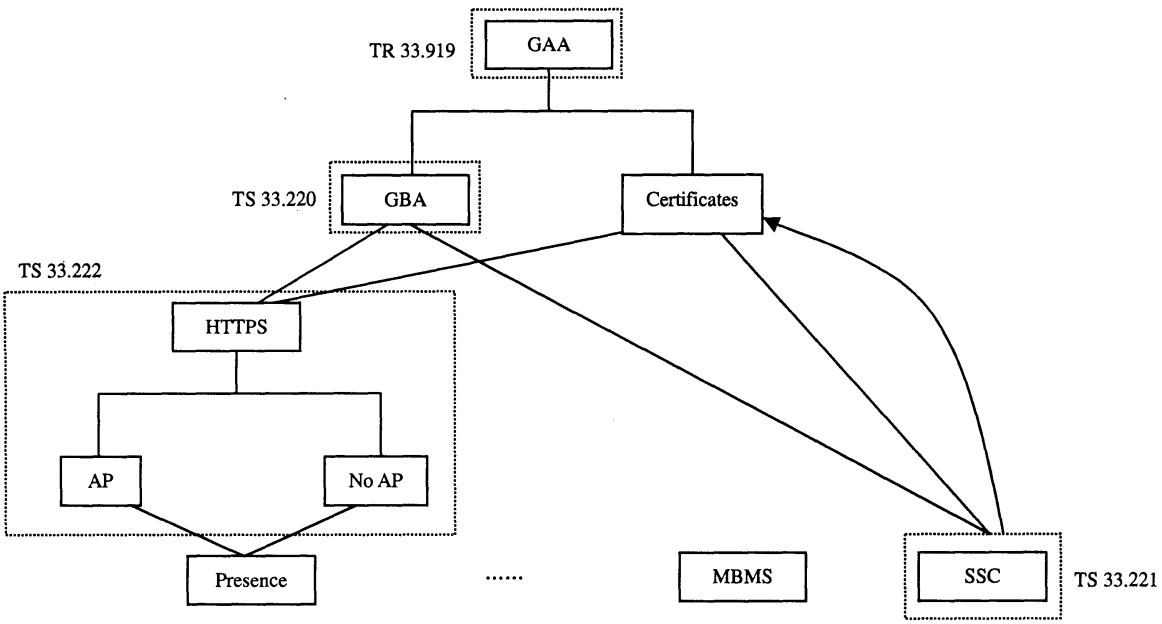


图5 GAA 结构模块内的相互关联

AP是TLS的端点，UE应能同时连接到位于一个AP后的多个不同AS。AP应能使用GAA的方式认证UE，也应能发送认证过的UE身份信息给AS。如果UE认证是基于一个共享秘密，那么AP的角色相当于GAA架构中的NAF。

使用AP的可能优势是：减少认证矢量（AV）的消耗，使SQN同步失败减小到最小，减少需要建立和维护TLS会话的数目。

4.4.5.2 无认证代理的 HTTPS

基于HTTP的AS也能在没有使用认证代理的情况下进行部署。在该情况下，HTTPS（或TLS）会话位于UE和AS之间。AS应能使用GAA的方式认证UE。如果UE的认证基于一个共享秘密，那么AS的角色相当于GAA架构中的NAF。

4.4.5.3 预共享密钥 TLS

HTTP用户和服务器可以基于UE和BSF在自举过程中生成的密钥作为GBA共享密钥互相认证。这个共享密钥应作为以后生成TLS会话密钥的主密钥，并且应作为认证功能的一部分作为拥有私钥的证明。具体过程参见3GPP TS 33.246 。

4.5 使用 GAA 的应用指南

GAA为AS或AP认证用户提供了不同的方法（即第5章中所描述的要求UE与BSF之间运行AKA、或使用基于用户证书的机制）。在GAA的框架中，一个AS能知道该用户的请求已经由认证代理AP认证。

本文所描述GAA的目的不是给移动应用强加任何一种认证机制，而是作为开发者部署的一种工具。使用GAA来取代为每一个应用设计和实现具体的认证机制，这样能为应用开发者节省开发时间。使用GAA的另一个好处是，继承GSM/UMTS的全球覆盖，应用开发者能提供全球覆盖的解决方案。

根据运营商的网络配置和策略，一个AS或AP能使用GAA提供的任何一种方式进行认证，更有甚者开发者能使用它们自己的且3GPP没规定过的用户认证机制。因此，前提条件是AS和AP应能决定使用GAA的哪些部分。

本章节试图给出关于选择认证机制的一些通用观点。认证机制的选择依赖于：

a）与需要认证的用户/服务器/应用/设备的要求/策略相关。也许需要双向认证（相互认证），但通常强调的是服务器认证用户。

b）用户档案里所定义的设备和业务的特征，用户能力和优先选择。

c）提供传输服务的网络策略，提供应用服务的服务提供商的策略。

与认证相关的需求/策略依赖于是否需要：

a）设备认证：设备真实有效而非克隆，即（U）SIM 认证质询响应。

b）完整性保护：UTRAN 接入的信令保护。GSM 的弱点是易受中间人攻击即攻击者能操作信令消息，如加密模式的命令。用于阻止这种安全威胁的一个方法是使用设备认证，并通过对指定信令消息进行加密的 MAC 码计算来达到完整性保护。

c）应用认证：有必要验证应用软件的真实性，具体例子见 TS 29.198-03 和 TS 29.199-01。然而应用认证超出了 GAA 的范围。

d）用户认证：对终端用户的认证。一种认证终端用户的方法是让设备/协议/应用在逻辑上（用户输入 PIN 码）或在物理上（插入和移走的策略）依赖于 USIM 可行性。在允许接入一个特定应用之前也许也要求输入一个 PIN 码。

e）交易认证和防抵赖性：对于一些使用移动设备进行的业务交易，有必要使用用户的私有密钥对此次交易进行数字签名，尤其是有必要进行防止交易抵赖，以便阻止：

—消息发送的否认，如“我从未发送过该消息”

—否认消息的内容，如“我说过你应出售，而不是买”

—否认消息发送的时间，如“我在另一个时间发送了该消息”

注： 类似于3GPP AKA的许多认证技术都是基于一个单一的由网络和用户共享的密钥，这对于发送者和接收者之间的认证是可行，但向第三方提供防抵赖的凭证则要求公钥技术，其对应的私钥由发送者拥有。

图6表示了设备和业务特征是如何影响从认证机制中选取一个特定的认证技术。

	认证类型		
客户端（设备）特征	设备（客户）认证	服务器认证	交易认证
PIN 码/口令	存储 PIN 码/口令	签名或口令	X
GAA：用户证书	客户端私钥，签名	签名	私钥，签名
GAA：GBA at UE	共享秘密（GBA），加密过的 MAC 码	共享秘密（GBA），加密过的 MAC 码或服务器私钥，签名	X
X：客户特征无法满足认证要求			

图6 认证特征比较

4.5.1 共享秘密和 GBA 的使用

GBA中使用共享密钥的一些实例：

—— 对称加密密钥和完整性密钥的分发，这些密钥能保证在 UE 和网络中服务器之间所运行的应用的安全。如用于保护一个应用安全并要求一个共享密秘的协议有 HTTP 摘要，共享秘密的 TLS 和 IPSEC；

—— 第三方应用的口令和 PIN 码的分发；

—— UE 和认证中心（CA）之间证书分发的保护。

4.5.2 证书的使用

UE和服务器证书的认证参见附录H。

标准分享网 www.bzfxw.com 免费下载

认证中使用证书的一些实例：

—— 验证终端用户的身份时；

—— 应用安全协议能与公私密钥对认证及用户证书（如 TLS）一起平稳工作时；

—— 有必要进行防止抵赖，及用户用自己私钥（类似于基于一个单一密钥的 3GPP AKA 认证技术，该单一密钥由网络和用户共享）对交易进行数字签名时，提供给第三方的防抵赖凭证要求使用公钥技术（其相应的私钥由发送者拥有）。

4.5.3 NAF 建议

4.5.3.1 概述

GBA可以应用不同类的Ua协议在很多不同种类的应用中使用。在本节，提出了一些建议帮助设计Ua协议。安全和业务交付可以从以下建议中受益，但是并不是所有的建议都适用于所有的应用，因此，每一个NAF的Ua协议都要确认这些建议是否可应用。

4.5.3.2 密钥生命周期管理

如果NAF有NAF自己定义的衍生密钥Ks_（ext/int）_NAF生命周期，但是它短于从BSF收到的缺省Ks的生命周期，（由于NAF自己的本地策略），为了避免UE和NAF不同的生命周期，并且对UE业务交付的连续性，至少要采取2种措施。一种方法是NAF可以通过Ua接口将密钥生命周期发送给UE，这样UE就可以在NAF定义的密钥生命周期过期之前发起一个新的自举过程。另一种方法是在NAF定义的密钥生命周期过期之前，NAF通过Ua接口指导UE发起一个新的自举过程。

4.5.3.3 用户身份确认

如果用户在Ua口发送一个或多个身份作为应用协议的一部分，并且如果NAF通过从BSF得到的业务特定的USS检查这些身份确实存在，确认这些身份确实属于签约用户，那么就能避免一些欺骗场景。只有当BSF和NAF都支持USS应用，并且NAF从UE发送过来的消息中提取身份信息时才可。

4.5.4 GAA 事件监控原则

GAA应用监控需要特定事件的记录。下面所列的事件，通过它们发生的接口分组，可以作为在网络节点实施监控的基本准则。

- Ub 接口：UE 和 BSF 通过 Ub 接口的自举。
- Ua 接口：

a）基于 bootstrapped 的 NAF 衍生密钥的 UE 和 NAF 认证；

b）签约用户公钥的注册；

c）运营商 CA 根证书的传递。

- Zn 接口：

a）NAF 衍生密钥的传送；

b）USS 的传送。

- Zh 接口：AV 和 GUSS 的传送。

注：这些表不一定是全部的。

4.6 GBA 的使用

本部分包括了3GPP规范和GBA扩展的一些应用实例。

4.6.1 GAA 和可信开放平台

TR33.905描述了GAA相关功能和与终端的互通。它描述了在Ub口与BSF服务器通信的终端的GAA服务器的关系，和通过相关设备驱动的UICC，作为终端应用的一部分的GAA用户与网络的通信，此网络是NAF服务器和在终端的GAA服务器获得的NAF特定GAA证书的网络。

4.6.2 2G GBA

TR33.920描述了基于SIM卡的共享密钥推送ME和NAF的应用。TS33.220主要描述GBA的3G USIM/ISIM的应用。2G GBA与使用USIM相似的认证方式和建立服务的管理方法。SIM卡应用的协议决定了整个系统得安全强度。因此，本部分描述的前期应用特性的解决方法旨在加强GSM的安全当使用2G GBA时。2G GBA不需要对现有规范作任何的修改。GBA_U只存在3G GBA中。

4.6.3 UICC 和终端的密钥建立

TS33.100描述了UICC和终端的密钥建立。UICC不是一个独立的设备，经常与终端放在一起使用。对于一些敏感的应用具有敏感数据传输，一般都将智能卡和终端分开。TS33.110提供了建立密钥的方法，来保证UICC和终端之间有一个安全的通道。

4.6.4 Liberty Alliance 和 GBA

TR33.980定义了GBA和Liberty Alliance的互通。GBA和Liberty Alliance身份联合与网络服务框架可以各自发展和配置。Liberty Alliance身份联合与网络服务框架为复杂的网络服务商务联系协议提供了简单单一的sign-on和会话管理。GBA为两个网络实体间基于GSM和UMTS的认证和密钥协商协议提供了共享密钥和证书的机制。TR33.980提供了GBA和Liberty Alliance框架的互通，并研究了GBA与Liberty Alliance Identity Federation Framework(ID-FF）,the Identity Web Services Framework(ID-WSF）对不同sign-on场景的互通方法。

4.6.5 MBMS 安全

TS33.246定义了TS33.220的应用。GBA用来为MBMS用户服务生成密钥。如果需要MBMS用户服务的保护，那么UE需要与BM-SC共享GBA密钥，BM-SC作为NAF。对于MBMS用户服务的MBMS服务密钥应保存，如果UICC能够管理MBMS密钥，就保存在UICC里，如果UICC不能管理，则保存在ME中。

5 GBA 过程

本章主要包括UE和BSF通过认证和密钥协商（AKA）进行自举的功能，和UE与NAF怎样使用bootstrap结果的总体架构和详细过程。

5.1 GBA 架构

3GPP认证基础设施包括了3GPP认证中心，用户业务身份模块（USIM）或 （ISIM）以及运行在它们中的3GPP认证及密钥协商协议，它是3GPP运营商非常有价值的资产。3GPP认证基础设施已经被公认为可以为网络侧的应用及用户建立共享密钥。因此，3GPP通过定义一个基于AKA协议的GBA，来提供基于应用层的对用户的认证。

5.1.1 参考模型

图7显示了一个简单的网络实体模型和它们之间的参考点，这些实体包含在自举过程中。

标准分享网 www.bzfxw.com 免费下载

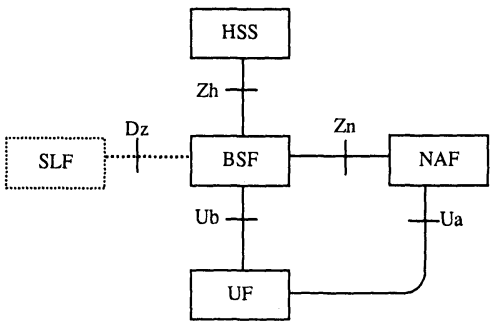


图7　自举的简单网络模型

图8显示了一个简单的实体网络模型，此时网络应用功能位于拜访网络。

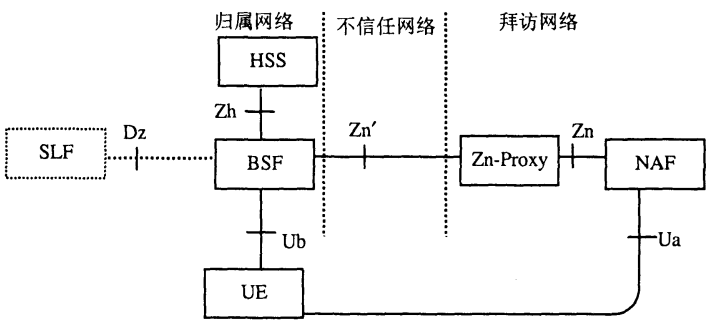


图8　拜访网络中自举

5.1.2　网络元素

5.1.2.1　BSF

通用自举服务功能（BSF）和UE应该利用AKA协议进行相互认证，并且建立会话密钥，这个密钥将会应用在UE和NAF之间。BSF通过利用附录A中的密钥衍生过程，来限制对于相关NAF的密钥资料的适用范围。密钥衍生过程在密钥资料的生存期内被多个NAF使用。根据BSF的当地策略来设置密钥资料的生存期。

BSF可以从HSS获得GBA的用户安全设置（GUSS）。

BSF可以保持一个列表，这个列表可以标记分配的NAF到了哪个NAF组。这个列表用来选择在GUSS里面哪一个应用相关的USS对于某个NAF是有效的。

注 1：运营商分配NAF到NAF组。NAF组在HSS里面定义的，并且所有属于同一个运营商的BSF都是应该平等的。由于这些网络元素属于同一个运营商的网络，所以NAF组的定义不必在协议里标准化。

注 2：NAF组可能是“归属”和“拜访”的。它允许BSF对于同一个应用发送USS，对于不同的NAF（比如拜访网络和归属网络的）要带有不同的授权标记。在拜访网络里（比如说）的NAF只是显示那些被请求的应用，但是它并不知道用户归属网络的分组。

5.1.2.2　NAF

自举结束以后，UE和NAF可以运行一些应用相关协议，在这些协议里面，消息的认证都是基于在UE和BSF相互认证过程中所产生的会话密钥。

针对NAF的一些假设：

1）UE和NAF之间以前没有安全关联。

2）NAF应该能够定位并且能够与用户的BSF进行安全的通信。

3）NAF在应用相关协议的运行过程中，应该能够获得在UE和BSF之间建立的一个共享密钥资料。

4）NAF应该能够通过BSF从HSS获得一个或多个应用相关的USSs，也可以不获得任何USS。

5）NAF应该能够根据本地政策来设定共享密钥资料的本地有效情况。

6）在GBA_U的情况，NAF应该能够通过应用本地策略或者在特定应用USS里的密钥选择指示决定使用哪一种密钥（即Ks_ext_NAF，Ks_int_NAF，或者两者）。如果NAF收到了特定应用的USS，其包括密钥选择指示，这种情况下应该覆盖NAF的本地策略。

7）NAF应该能够检测共享密钥资料的生存期和本地有效条件。

注： 如果不采取附加的措施GBA不能保证密钥Ks（_int/ext）_NAF的刷新性，即不能保证密钥没有在以前的Ua协议的执行中使用过。UE和NAF可以采取以下附加的措施来保证GBA中的密钥的刷新性：

① 在衍生一个新的 Ks_NAF 之前，再执行一次 Ub 协议（产生一个新的 Ks）。

② 存储以前用过的密钥 Ks（_int/ext）_NAF，或者相应的密钥标识符 B-TID，直到它们生存期满。

支持 Ua 协议的一个 UE 和一个 NAF，在需要的情况下，需要采取相应的措施来避免重放攻击，因为 Ua 协议在无连接运行中不能防止重放攻击。

5.1.2.3 Zn-Proxy

当UE被连接到一个外地网络的NAF时，这个拜访的NAF需要利用NAF网络的Zn-Proxy与用户的BSF（归属网络的BSF）进行通信。

注意：Zn-Proxy功能可能作为一个单独的网络元素来执行，或者作为拜访网络中任意网元的一部分去执行Diameter/HTTP proxy功能（这种网元的例子可以是拜访网络NAF所属网络中的BSF，其拜访网络属于一个AAA服务器或者一个HTTP服务器）。

Zn-Proxy的一般要求：

1）Zn-Proxy 应该能够在拜访 NAF 和用户的归属 BSF 之间起到代理的作用。

2）Zn-Proxy 应该能够定位用户的归属 BSF 并且可以通过安全信道与它通信。

3）Zn-Proxy 应该能够确定拜访的 NAF 有权利参与 GBA，并且应该能够向用户归属 BSF 提供 NAF DNS 名称。Zn-Proxy 应该能够向 BSF 确保拜访的 NAF 有权请求 GBA 相关用户描述文件，这个请求也包含在 NAF 请求中。

4）Zn-Proxy 的物理安全级别不能低于与它交互的 NAF 的最高级别。

5.1.2.4 HSS

所有的用户安全设置（USS），即GUSS，都存储在HSS中。在一个用户具有多个订阅业务（比如在UICC上具有多个ISIM或者USIM应用）的情况下，HSS可以会包含一个或者多个GUSS，这些GUSS可以映射到一个或者多个私有身份（即IMPI，IMSI）。每一个GUSS应与一个或多个私有身份映射，但是每一个私有身份只能与零个或一个GUSS相映射。

HSS的要求：

1）HSS 能够提供 GUSS 的永久性存储。

2）GUSS 应该以这样的方式来定义，即不同运营商对于标准的应用描述文件的交互是可能的。

3）GUSS 应该以这样的方式来定义，即运营商应用相关和已经存在的应用描述文件的扩展不需要这些元素的标准化就可以支持。

4）GUSS 应该包含应用相关 USSs，这些 USSs 包含着与一个或者多个应用的认证和认证信息相关的

标准分享网 www.bzfxw.com 免费下载

参数，这些应用是由 NAF 发起的。任何其他类型的参数在应用相关 USS 里面是不允许的。

注 1：NAF可以从它的本地数据库中直接获得签约用户的描述文件数据而不需要HSS的参与。

注 2：一种从GUSS里临时取消特定应用USS的可能是，如果签约用户临时取消了业务，那么HSS可以临时把特定应用的USS从GUSS里移去。这种操作BSF的GUSS不改变，只有当现在自举会话超时会更新，或者当一个新的修改过的GUSS携带着AV从HSS里取出时建立了一个新的自举会话，那么原来的GUSS会被覆盖。

5）GUSS 应该包含 BSF 应用所需的参数：

— 用户使用的 UICC 的类型；（是否支持 GBA_U 功能）

— 用户相关密钥生存期；

— 可选的时间戳，其指示 GUSS 最后一次被 HSS 修改的时间。

注 3：这些参数都是可选的，如果用户的GUSS里面不存在这些参数或者用户没有GUSS，那么BSF就可以利用在BSF本地策略中的缺省值，这个本地策略是由一个MNO自己定义的。

6）HSS 应该能够分配应用相关的 USS 到 NAF 组。可能出现不同的 USSs 针对相同的应用，但针对不同 NAF 组的情况。GUSS 中对于 USS 数目的限制依赖 NAF 组的业务。

7）对于某个应用，如果没有 NAF 组定义，那么对于每个应用至多有一个 USS 存储在 GUSS 里面。

8）对于某个应用，如果 NAF 组定义了，那么对于每个应用至多有一个 USS 和 NAF 组被存储在 GUSS 里面。

9）在 HSS 中 NAF 组的定义和所有属于同一个运营商的 BSF 都应该是平等的。

5.1.2.5 UE

UE所必需的功能：

1）支持 HTTP DIGEST AKA 协议；

2）在自举中能够应用 USIM 和 ISIM 的能力；

3）当 USIM 和 ISIM 都可用的情况下，具有选择在自举中使用哪一个的能力；

4）ME 上的一个 Ua 应用具有向 ME 上的 GBA 功能指示出在自举中使用的 UICC 应用的名字或者类型的能力；

5）利用 CK 和 IK，产生新的可以在 Ua 接口协议上和应用一起使用的密钥资料的能力；

6）NAF 应用相关协议的支持（可以参考第 6 章）。

一个支持 GBA 的 ME 应该支持 GBA_U 和 GBA_ME。

5.1.2.6 SLF

SLF：

1）由BSF通过Zh接口操作向其询问以得到包括要求的签约用户特定数据的HSS的名字；

2）BSF通过Dz接口连接。

在单一的HSS环境里不需要SLF。当BSF被配置或被管理使用预定义的HSS时，不要求使用SLF。

5.1.3 自举框架和参考点

5.1.3.1 参考点 Ub

参考点Ub在UE与BSF之间。参考点Ub提供UE与BSF之间的相互认证。它允许UE基于3GPP AKA基础设施bootstrap会话密钥。

HTTP DIGEST AKA协议（在RFC 3310中详细说明），用在参考点Ub上。它是基于3GPP AKA TS 33.102协议的。对于USIM的接口在TS 31.102中有详细说明，对于ISIM的接口在TS 31.103中有详细说明。

5.1.3.2 参考点 Ua

参考点Ua承载应用协议，利用UE与BSF之间协商的密钥资料来保证其安全，这个密钥资料是在参考点Ub上运行HTTP DIGEST AKA的结果。举个例子来说，在支持用户证书协议（第6章）的情况下，它是一个允许用户从NAF中请求证书的一个协议。在这种情况下，NAF就是一个PKI入口。

详见附录E。

5.1.3.3 参考点 Zh

参考点Zh用在BSF和HSS之间，它允许BSF从HSS里面获得必要的认证信息和所有的GBA用户安全设置。对于3G认证中心的接口是HSS内部的，所以不需要作为这个架构的一部分来进行标准化。

5.1.3.4 参考点 Zn

参考点Zn被NAF用来获得密钥资料，这些密钥资料是在前一次在UE与BSF之间的参考点Ub上运行HTTP DIGEST AKA协议协商的结果。如果NAF请求，这个接口也可以用来从BSF中获得应用相关的用户安全设置。

5.1.3.5 参考点 Dz

参考点Dz应用在BSF和SLF之间，其允许BSF得到包括要求的签约用户特定数据的HSS的名字。

5.1.4 自举的原理与要求

下面的原理与要求对于自举过程是可适用的：

1）自举功能不能依赖特定的 NAF；

2）实现自举功能的服务器需要被本地运营商所信任，才能去处理认证向量；

3）实现 NAF 的服务器需要被本地运营商所信任，才能去处理衍生的密钥资料；

4）在运营商的本地网络和拜访网络都需要支持 NAF；

5）这个架构不能排除在第三方网络中对网络应用功能的支持；

6）已经存在的协议和基础设施需要得到最大限度的重新利用；

7）为了确保最大限度的适用性，所有相关的协议都应运行在 IP 之上；

8）要防止攻击者利用 NAF 的安全漏洞去成功的攻击其他的 NAF，这里所涉及的 NAF 都使用 GBA；

9）要防止攻击者利用 Ua 口上一个安全协议存在的漏洞来实现对 Ua 口上另外的安全协议的成功攻击。

5.1.4.1 接入的独立性

自举过程是独立接入的。并且自举过程需要UE的IP连接。

5.1.4.2 认证方式

如果没有一个有效的蜂窝网签约信息，UE与BSF之间的认证是不可能的。认证应该基于3GPP AKA协议。

5.1.4.3 漫游

漫游时的要求：

1）漫游用户应该能够利用归属网络中的自举功能。用户应该能够利用在拜访网络的网络应用功能（NAF）；

标准分享网 www.bzfxw.com 免费下载

2）归属网络应该能够控制它的用户能否被授权使用拜访网络的服务。

5.1.4.4 参考点 Ub 上的要求

参考点Ub的要求：

1）BSF 应该能够认证 UE；

2）BSF 和 UE 应该能够基于 AKA 进行双向认证；

3）BSF 应该能够发送自举事务标识符到 UE；

4）UE 和 BSF 应该建立共享密钥；

5）BSF 能够通知 UE 密钥资料的生存期；BSF 通过 Ub 发送的密钥生存期将会指示生存期满。

注：这并不能排除UE根据UE的本地策略在生存期满之前刷新密钥。

5.1.4.5 参考点 Zh 上的要求

参考点Zh的要求：

1）相互认证，可以提供保密性和完整性；

注 1：如果BSF和HSS都在同一个运营商的网络，这个要求可以通过物理或者专有的安全方式来满足。

2）BSF 应该能够发送用户的自举信息请求；

3）可选地，BSF 可以有能力给 HSS 发送签约用户 GUSS 的时间戳（时间戳选项）；

4）HSS 应该能够向 BSF 一次发送一个 3GPP AKA 认证向量；

5）HSS 应该能够根据安全目的的需要向 BSF 发送完全的签约用户的 GUSS。可选地，HSS 可以有能力指示 BSF，BSF 是否已经有了基于 GUSS 时间戳的最近一次的 GUSS 拷贝（时间戳选项）。

注 2：如果用户的GUSS在HSS进行了更新，更新的GUSS不会立即传送到BSF。作为自举过程的一部分，当BSF下次通过Zh从HSS获取认证向量和GUSS的时候，BSF中的GUSS会被更新。

6）没有与自举相关的状态信息需要在 HSS 保存；

7）通过参考点 Zh 的所有过程都是由 BSF 初始化的；

8）与 HSS 的不同接口的数目应该保持最少。

5.1.4.6 参考点 Zn 上的要求

参考点Zn的要求：

1）相互认证，可以提供保密性和完整性。

2）如果 BSF 和 NAF 在同一个运营商的网络内，基于参考点 Zn 的 DIAMETER 协议应该根据 NDS/IP 受到保护。

3）如果 BSF 和 NAF 不在同一个运营商的网络内，在 Zn-Proxy 和 BSF 之间的基于参考点 Zn′的 DIAMETER 应该利用 RFC 2246 中的 TLS 来保证安全。

注 1：附录D和附录C详细说明了TLS描述文件。

4）基于 Zn/Zn′接口的 HTTP 协议应该使用 RFC 2246 中的 TLS 来保护。

注 1b：附录D详细说明了TLS描述文件。

5）BSF 应该保证发出请求的 NAF 能够被批准去获得密钥资料和请求的 USS。

6）NAF 应该能够发送密钥资料请求到 BSF，BSF 包含着 UE 相关请求使用的 NAF 的公共主机名。BSF 应该能够保证 NAF 可以获得批准去使用这个主机名，比如说：UE 与 NAF 通信时使用 FQDN。

7）BSF 应该能够发送密钥资料到 NAF。

8）NAF 应该能够从 BSF 中有选择性的获得应用相关的 USS，NAF 能够获得什么 USS 决定于 BSF 的策略和 NAF 通过参考点 Zn 的请求消息中的指示。

9）NAF 应该能够向 BSF 指示出它所需要的 USS 用于一个或者多个应用。

注 2：如果一些应用只需要应用相关的USS的一个子集，比如说只需要一个IMPU，那么NAF就可以从来自BSF的完整USS中选择这个子集。

10）BSF 应该能够对每一个 NAF 或每一个应用被配置，基于

— 是否签约用户的私人身份，即 IMPI，可能发送给 NAF；

— 是否一个特定的 USS 可能发送给 NAF。

注 3：当需要决定使用哪种用户身份发送给NAF时需要考虑到隐私问题。如果希望服务连续性，那么BSF可以配制成发送IMPI（但是没有用户假名）。如果BSF不在USS里发送IMPI，IMPU或者假名，那么UE对于NAF是保持匿名的，或者更准确地说，B-TID是作为一个临时用户标识的。这可以引起NAF不能提供服务的连续性，因为当UE使用一个新的B-TID进行自举并联系NAF时，NAF需要用户身份来为Ua会话更新密钥。如果需要用户身份，NAF可以请求USS，BSF可以配制成在USS里发送用户假名，而不是IMPI。

11）如果一个 NAF 向 BSF 请求 USS，但是用户的 GUSS 里面不存在 USS，倘若 BSF 本地策略的条件满足了，这就不会引起一个错误。BSF 应该仅将要求并找到的 USS 发送给 NAF。

12）按照下面的描述来配置一个本地策略是可能的：对于一个相关请求的 NAF，BSF 可能需要一个或者多个应用相关的 USS 在这个用户相关的 GUSS 中，如果条件没有满足，就要拒绝来自 NAF 的请求。为了满足这个本地策略，NAF 不需要通过 Zn 参考点来请求 USS，这些 USS 是 BSF 要求在 GUSS 里面存在的，只需要 BSF 在本地查询 USS 就已经足够了。在发出请求的 NAF 没有要求 USS 的情况下，配置 BSF 也是可能的。

注 4：对于更多的有关本地策略应用的信息见3GPP TS33.220附录J。

13）BSF 应该能够向 NAF 指示出自举的时间和密钥资料的生存期。BSF 通过 Zn 传递的密钥生存期，应该与 BSF 通过 Ub 传递给 UE 的密钥资料的生存期一样。

注 5：这并不能排除NAF在生存期满之前根据本地策略来更新密钥。

注 6：HSS里面的GUSS中的一个或者多个USS（已经发送到NAF了）被更新，只有当NAF下次从BSF请求USS时，更新过的USS才对NAF起作用（假设BSF已经通过Zh参考点更新了用户的GUSS）。

14）BSF 应删除任何显示 NAF 组从 USS 到 NAF 的特征。

15）NAF 应该能够指示 BSF 在 Ua 口安全协议的协议标识，BSF 要传送 NAF-ID 给 BSF。

5.1.4.7 自举事务标识的要求

Bootsrapping事务标识（B-TID）通过参考点Ua、Ub和Zn将用户身份和密钥资料绑定。

B-TID的要求：

1）B-TID 应该是全局唯一的；

2）B-TID 应该作为一个密钥标识符来使用，应用在 Ua 参考点上；

3）NAF 应该能够从 B-TID 中检测到 UE 的归属网络及相应的 BSF。

注 1：NAF在密钥无效之后，要删除那些符合删除条件的安全关联。

注 2：UE和NAF之间使用GBA还是非GBA认证，不能产生冲突，比如说在同一个命名空间。这种潜在的冲突不能通过通用的方式来解决，因为它依赖于相关的协议和UE与NAF之间所使用的认证机制。这超出了本规范的范围。

标准分享网 www.bzfxw.com 免费下载

对于在UE和NAF之间使用的HTTP摘要认证的例子，下面的这种使用方式也是可能的：〈用户名，密码〉对在一个域内必须是唯一的。由于NAF控制域名，所以它必须确保只有基于域的GBA才能以保留的3GPP域名来进行命名。在特殊的情况下，NAF 要在GBA域内允许基于非 GBA的认证，它必须确保没有基于GBA认证之外的用户使用B-TID格式的用户名。

5.1.4.8 UICC 的选择和相关密钥的要求

UICC的选择和相关密钥的要求参见附录B。

当能够执行AKA的UICC中存在多个应用时，那么ME应该按照下述的优先级选择UICC的一个应用去执行本部分规定的GBA的流程。

UE 决定哪个 UICC 应用是相关的。

（1）ME 上需要 Ks_NAF 的应用可以向 GBA 功能指示出 UICC 应用的类型和名字：no preference，USIM，ISIM，或者 UICC 应用的“Label”（在 TS 31.101 中定义）。

注 1：Ua应用的规范可以要求只使用USIM（如在MBMS情况时），或者ISIM。

注 2：用户或者运营商可以根据“Label”的指示对特定UICC应用使用Ua应用。这可以由用户或者运营商在ME中的Ua应用配置。

一个Ua应用可以要求对一个Ua应用的例子在Ub协议的开始和后续步骤中使用相同的UICC应用，来保证在一个Ua应用会话持续在几个Ub协议的过程中IMPI不改变。在这种情况下，Ua应用应请求GBA在Ub口运行UICC应用，此应用由相应的“Label”或IMPI指示，取决于那一个指示可用。如果都可用，那么应使用IMPI指示GBA功能使用哪种UICC应用。

如果 ME 的应用指示出 UICC 应用的“Label”，下面的 b）将会执行。

如果 ME 的应用指示出 UICC 应用的类型是下面的：

① UICC 上的 USIM；跳过下面的步骤 b），只考虑步骤 c）和步骤 d）中的 USIM 应用。

② UICC 上的 ISIM；跳过下面的步骤 b），只考虑步骤 c）和步骤 d）中的 ISIM 应用。

如果 ME 上的应用不能指示出优先级，将会跳过下面的步骤 b），而从步骤 c）开始进行选择执行。

（2）如果在步骤 a）中显示“Label”，至多，一次只能有一个 USIM 激活。因此，如果在 Ua 应用里的“Label”指示的 USIM 和现在激活的 USIM 应用不同的话，ME 会拒绝这个请求。

如果 Ua 应用指示给 GBA 支持功能一个不同于当前激活的 ISIM 应用的 ISIM，那么 ME 不应该终止当前激活的 ISIM 应用，但是当“Label”指示激活 ISIM 应用，ME 应该按照 5.1.4.8.1 的步骤操作，因为 UE 允许同时有几个激活的 ISIM。

（3）如果在步骤 a）没有“Label”指示，并且有 UICC 应用激活：

如果一个首选的 UICC 应用类型被指示，但是没有这种类型的 UICC 应用被激活，那么按照步骤 d 进行。

如果一个首选的 UICC 应用类型被指示，并且也有这个首选类型的激活的 UICC 应用，那么，GBA 功能就要选择：

① 如果这个首选的 UICC 应用类型是 USIM，那么就选择激活的 USIM；

② 如果这个首选的 UICC 应用类型是 ISIM，并且只有一个 ISIM 被激活，那么就选择这个激活的 ISIM；

③ 如果这个首选的 UICC 应用类型是 ISIM，并且有多于一个 ISIM 被激活，那么 GBA 功能就要给终端用户显示一个 UICC 应用选择对话（列表包括 UICC 上所有激活的 ISIM 应用的应用列表上的

“Labels”），终端用户从中选择 UICC 应用；如果没有对话，那么 GBA 功能选择一个激活的 ISIM。

如果没有参考，并且有多于一个 UICC 应用，那么 GBA 功能就要给终端用户显示一个 UICC 应用选择对话（列表包括所有激活的 UICC 应用的应用列表的“Labels”），终端用户从中选择 UICC 应用；如果没有对话，有一个激活的 USIM 存在，那么 GBA 功能就要选择激活的 USIM 应用，否则选择任意激活的 ISIM 应用。

如果没有参考，并且只有一个激活的 UICC 应用，那么 GBA 功能选择这个激活的 UICC 应用。

（4）如果步骤 a）没有“Label”，并且没有 UICC 应用激活，或者没有属于首选 UICC 应用类型激活的 UICC 应用：

① 如果只有一个 UICC 应用，GBA 功能就会选择这一个；

② 如果这里有多于一个的 UICC 应用，GBA 功能将会给终端用户显示一个 UICC 应用会话（列表中包含 UICC 应用中的所有“Label”），用户可以选择一个应用；如果有一个首选的 UICC 应用类型被指示，并且 UICC 上有这种类型的 UICC 应用，那么列表只包括这种类型的 UICC 应用，否则，列表包括所有的 UICC 应用。如果没有对话，那么 GBA 功能选择首选类型的最后一次被选择的 UICC 应用（即，根据参考选择最后一次选择的 USIM 或者最后一次选择的 ISIM），如果可能的话。在 Ua 应用没有参考且 USIM 和 ISIM 都在 UICC 上时，最后一次选择的 USIM 被选择。

按照步骤 5.1.4.8.1 操作。

a）如果步骤 a）指示的 UICC 应用类型和步骤 c）和/或 d）使用的是 ISIM，但是没有 ISIM 可以选择，那么 UICC 应用类型 USIM 重复步骤 c）和/或 d）；否则选择过程失败。

注 3：步骤e）实现使用UICC上的USIM应用代替ISIM。

b）如果已经存在了从 UICC 应用中产生的密钥 Ks，UE 将会从这个密钥中产生 Ks_NAF。

c）如果不存在这个密钥 Ks，UE 首先要运行包含 UICC 应用的 Ub 协议，然后到第二步。

d）如果一个 USIM 被选择了，就可以从 USIM 中存储的 IMSI 中获得 IMPI，这个 IMPI 可以通过 Ub 应用在协议中。

注 4：严格的讲，IMPI和从IMSI中导出IMPI（在TS23.003中）只在IMS的上下文中定义。为了完成这个规范的目的，虽然用户没有IMS订阅，但从IMSI中获得的标识（在23.003详细说明）称为IMPI。

e）如果 ISIM 被选择了，储存在 ISIM 中的 IMPI 将会通过 Ub 在协议中使用。

不管 UICC 应用被成功选择还是被终结，这个选择 UICC 应用的规则都是可以重复使用的，因此，GBA 选择的 UICC 应用可以改变。

注 5：任何时候，都至多有一个UICC应用在执行GBA功能。

5.1.4.8.1 GBA 功能 UICC 应用激活过程

UICC应用激活在TS31.101中定义。

注：作为UICC应用（USIM或者ISIM）激活过程的一部分，UICC可以要求用户确认，如PIN接入。

如果一个新的UICC应用激活失败，则GBA功能要将此指示给Ua应用。

5.1.4.9 参考点 Ua 的要求

参考点Ua的一般要求：

1）UE 和 NAF 应该可以使用基于 GBA 的共享秘密来保证参考点 Ua 的安全；

注：确切的保证参考点Ua安全的方法依赖于在参考点Ua上使用的应用协议。

标准分享网 www.bzfxw.com 免费下载

2）在 GBA_U 的情况，如果 2 种密钥都可以使用，那么 UE 和 NAF 应该能够协商使用哪一种密钥（即 Ks_ext_NAF 或 Ks_int_NAF 或者两者）作为基于 GBA 的共享密钥。

UE 和 NAF 有两种方法达成一致使用哪种密钥 Ks_ext_NAF 或 Ks_int_NAF 或者两者：

a）通常情况下，Ua 口使用的协议可以使用不同的应用（如 HTTPS），协议应该可以指示使用哪一种密钥。

b）在特定的情况下，协议是针对特定应用的（如 MBMS 的 MIKEY 协议），可以基于固有知识判断：

① Ua 口的任何安全协议都应该伴随着 Ua 安全协议标识；

② NAF 应该能够指示 UE 要使用基于 GBA 的共享密钥；

③ NAF 应该能够指示 UE，现在的共享密钥过期，UE 要与 NAF 使用新的共享密钥；

④ 当在 Ua 应用规范中没有特别提到时，NAF 衍生密钥 Ks_（ext/int）_NAF 的缺省生命周期与 Ks 的相等。NAF 衍生密钥 Ks_（ext/int）_NAF 的生命周期不能长于其相应的 Ks 的生命周期。如果 NAF 中有 Ks_（ext/int）_NAF（或者密钥衍生材料）的生命周期，由于 Ua 口规范有自己的生命周期值，或者由于 NAF 对密钥衍生材料的本地策略，造成了这个生命周期与从 BSF 收到的 Ks 的生命周期不同，那么 NAF 应该要始终选择这 2 种密钥生命周期中的最小值。

⑤ UE 和 NAF 可以对于 Ua 口特定需要适应密钥材料 Ks_（ext/int）_NAF。此内容超出本部分范围。当 Ua 口应用规范没有特别指示时，缺省密钥材料的生命周期应该等于 Ks_（ext/int）_NAF 的生命周期。密钥材料的生命周期不应该长于相应的 Ks_（ext/int）_NAF 的生命周期。如果 NAF 中有 Ks_（ext/int）_NAF（或者密钥衍生材料）的生命周期，由于 Ua 口规范有自己的生命周期值，或者由于 NAF 对密钥衍生材料的本地策略，造成了这个生命周期与从 BSF 收到的 Ks 的生命周期不同，那么 NAF 应该要始终选择这 2 种密钥生命周期中的最小值。

5.1.4.10 参考点 Dz 上的要求

BSF和SLF之间的接口用来得到包含签约用户信息的HSS的地址。这个接口在单一的HSS环境中不要求。

5.1.4.11 GBA 密钥和参数控制的要求

当提到GBA密钥时，以下的密钥被涉及到：KS和从Ks衍生的NAF密钥。当提到NAF衍生密钥时，以下密钥被涉及到：Ks_ext/int_NAF（在GBA_U时）和Ks_NAF（在GBA_ME时），和任意从这些密钥衍生的密钥。Ks_（ext/int）_NAF指的是在GBA_U时的Ks_ext/int_NAF和GBA_ME时的Ks_NAF。Ks_（ext）_NAF指的是GBA_U时的Ks_ext_NAF和GBA_ME时的Ks_NAF。

ME应该删除GBA相应的密钥（即Ks和NAF衍生密钥）和相应的NAF_IDs，B-TID，Ks_（ext/int）_NAF生命周期和Ks生命周期，以及从Ks_（ext）_NAF衍生的密钥的生命周期，当以下条件之一满足时：

a）当ME有电时移出UICC；

b）当ME开机时发现有另一个UICC插入。这种情况，ME需要在稳定存储里保存最后一次插入的UICC身份，用来与新插入的UICC身份进行比较；

c）ME开机时发现没有UICC卡插入。

注：在开放平台上的应用满足此需求的一种可能是，如果密钥在开启和关闭应用时密钥是否被删除。当ME系统检测到上述条件时，它可以关闭应用来强制删除密钥。在开启时的密钥删除可以保证当不规则的关机或当关机时UICC移出时

的密钥删除。

当Ks的密钥生命周期过期时，ME应删除与此Ks对应的所有GBA密钥（即Ks和NAF衍生密钥）和相对应NAF_ID，B-TID，Ks_（ext/int）_NAF生命周期和Ks生命周期，以及从Ks_（ext）_NAF衍生的密钥的生命周期。

在GBA_ME的情况下，当ME断电时，Ks需要从ME中删除。当ME断电时，NAF衍生密钥（即Ks_（ext）_NAF和任何从其衍生的密钥）可以从ME中删除。如果ME在断电时不删除这些NAF衍生密钥，那么NAF衍生密钥（即Ks_（ext）_NAF和任何从其衍生的密钥）和NAF_IDs，B-TID，Ks_（ext）_NAF生命周期和从Ks_（ext）_NAF衍生的密钥的生命周期应该保存到稳定存储里。

如果NAF衍生密钥保存在稳定的存储里，那么当ME又开机时，ME可以需要保证同一个UICC应用被选择以保证是同一个Ua应用，为了允许NAF衍生密钥（即Ks_（ext）_NAF和任何从其衍生的密钥）的重用。因此，ME应在稳定存储里保存IMPI。如果当ME开机时，对Ua应用不能选择相同的UICC，那么ME应删除在稳定存储里保存的与IMPI相关的NAF衍生密钥。

无论何时UICC应用中断了（见5.1.4.8节），Ub口协议建立的共享密钥Ks应该删除。

注：这种情况下，Ks被删除了，但是相同的UICC还存在（即不是条件2，3，4满足），Ua应用能够继续使用NAF衍生密钥（Ks_（ext/int）_NAF）直到Ks生命周期过期。

5.1.5 过程

这一节详细介绍了自举过程，这个过程将会被各种应用所使用。它包含AKA认证和密钥资料的产生过程。

5.1.5.1 自举的初始化

在 UE 和 NAF 进行通信之前，UE 和 NAF 首先需要协商是否需要使用 GBA。当 UE 要与 NAF 进行通信，但是 UE 不知道 NAF 是否需要通过 GBA 方式产生共享密钥，并且 UE 可在在该条连接请求中，指示自己是否是 2G 用户。这时，UE 就需要进一步与 NAF 交互获取指示。

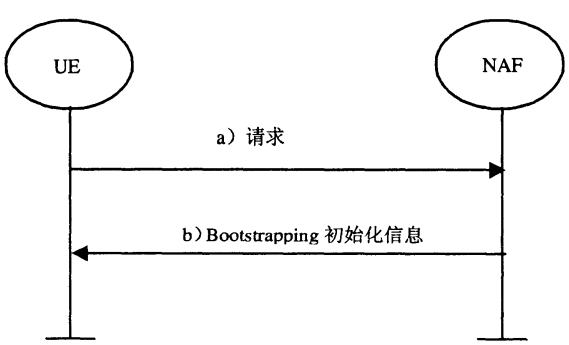


图9 自举的发起

a）UE 通过 Ua 参考点发起与 NAF 的通信。

b）如果 NAF 需要使用通过 GBA 方式产生的共享密钥，NAF 回复一个自举初始化信息。这种通知的方式取决于相关的参考点 Ua，在相关的第三阶段的规范中详细说明。

5.1.5.2 自举过程

UE与NAF通信，并且知道需要一个自举过程，那么它将首先进行自举认证。另外，只有当UE接收到NAF发送回来的自举初始化消息或者来自NAF的自举协商指示后，再或者当UE中的密钥生存期满的时候，才执行自举认证。

标准分享网 www.bzfxw.com 免费下载

注 1：在规范TS 33.102中的AKA协议和RFC 3310的HTTP DIGEST AKA协议中的主要的步骤，为了读者的方便而在下图中重复了。如果存在任何潜在的冲突，以TS 33.102和 RFC 3310的规范内容为准。

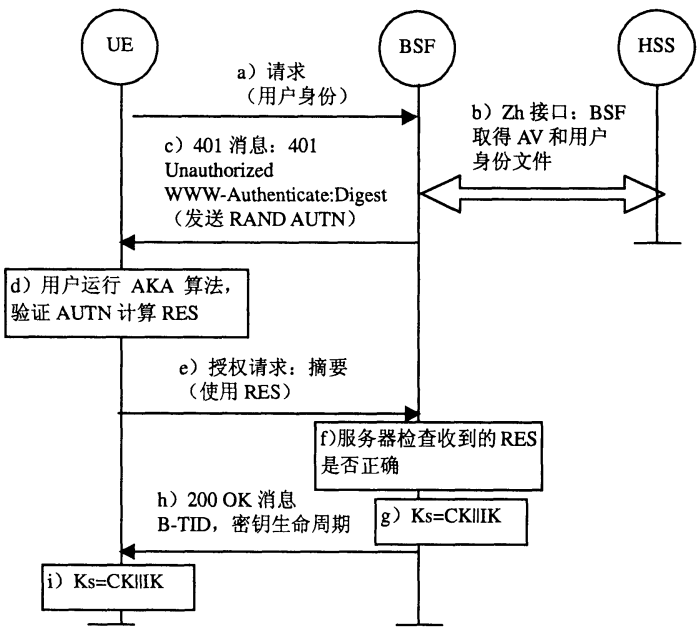


图10 自举过程

a）UE 向 BSF 发送 HTTP 请求，包括用户的身份信息 B-TID，如果没有有效的 B-TID，则发送 IMPI。

b）BSF 通过参考点 Zh 从 HSS 中获得 GBA 用户的全部安全参数设置和一个认证向量（AV，AV = RAND||AUTN||XRES||CK||IK）。

如果 BSF 在上一次自举过程应用时间戳选项，并且有从 HSS 得到的签约用户的本地 GUSS 的拷贝，这个 GUSS 包括时间戳，那么 BSF 可以在请求信息里包括 GUSS 时间戳。得到时间戳后，如果 HSS 应用时间戳选项，那么 HSS 将它与储存在 HSS 里的 GUSS 时间戳比较。在这种情况下，当且仅当 HSS 作了比较并且时间戳相等时，HSS 将“GUSS 时间戳相等”指示发送给 BSF。在其他情况下，HSS 把 GUSS（如果存在）发送给 BSF。如果 BSF 接收到“GUSS 时间戳相等”指示，它就存储 GUSS 的本地拷贝。其他情况，BSF 删除 GUSS 的本地拷贝，并且存储得到的 GUSS（如果发送）。

注 2：在有多个HSS的环境里，优先于步骤2，BSF可以通过询问SLF得到储存用户签约的HSS地址。

c）BSF 通过 401 消息把 RAND 和 AUTN（不发送 CK，IK 和 XRES）发送给 UE。

d）UE 检查 AUTN 来认证网络；UE 还计算出 CK，IK 和 RES，从而在 BSF 和 UE 内产生会话密钥 IK 和 CK。

e）UE 发送另一个 HTTP 请求到 BSF，其中包含着摘要 AKA 响应（使用 RES 计算出来的）。

f）BSF 通过摘要 AKA 响应来对 UE 进行认证。

注 3：在“AKAv1”中的HTTP摘要AKA的密码是二进制。

g）BSF 通过 CK 和 IK 来产生密钥资料 Ks。根据 base64 编码规则来对第三步产生的 RAND 和 BSF 服务器名进行编码，并以 NAI 的格式来产生 B-TID 值，即 base64encode（RAND）@BSF_servers_domain_name。

h）BSF 发送 200 OK 消息到 UE 通知认证成功，该消息中包含 B-TID。除此之外，在这个 200 OK 消息中还要包含这个密钥 Ks 的生存期。在 UE 中也根据 CK 和 IK 来产生密钥资料 Ks。

注 3：如果步骤1采用用户身份标识B-TID，则步骤8中BSF发送给UE的B-TID需要加密发送。

i）UE 和 BSF 应该利用 Ks 产生密钥资料 Ks_NAF。利用 Ks_NAF 来保证参考点 Ua 的安全。

Ks_NAF 根据下面的公式来计算 Ks_NAF = KDF （Ks，"gba-me"，RAND，IMPI，NAF_Id），KDF 是在附录中说明的密钥衍生函数，密钥衍生参数由用户的 IMPI，NAF_Id 和 RAND 组成。NAF_Id 的结构是：NAF_Id=NAF 的 FQDN||Ua 安全协议标识。KDF 也应该在 ME 内执行。

注 4：如果一个NAF拥有有相同FQDN和Ua安全协议标识的2个或多个应用，那么它们应共享相同的NAF衍生密钥。这会引起所谓的"two-time pad"，会导致这些应用的安全妥协的情况。这可以通过分别进行自举过程或者应用的特定方法避免，这超出了本标准范围。

在 UE 和 BSF 里要保持基于 NAF 名的一致密钥衍生，至少应该满足以下几个前提条件：

（1）在 DNS 内，NAF 只有一个域名。比如说，不能存在两个不同的域名对应同一个 NAF 的 IP 地址。这要通过管理方式才能完成。这个前提条件在 3GPP 内并不是很特殊的，因为这在其他地方也是必须的，比如说在没有使用通配符和多名证书的 TLS V1.0。

（2）NAF 的每个 DNS 入口对应着不同的 IP 地址。NAF 向所有的 IP 地址作出响应。每个 IP 地址通过 NAF 配置绑定到相应的 FQDN。FQDN 使用从 IP 地址中推出的 NAF 进行密钥衍生。

（3）Ua 使用传输主机名（UE 使用的 NAF 的 FQDN）到 NAF 的协议（例如带有强制主机请求头域的 HTTP/1.1）。这需要 NAF 检查主机名的有效性，从而在与 UE 所有的通信过程中都使用这个名字，还要将这个名字传送给 BSF，达到正确衍生出 Ks_NAF 的目的。

在 TLS 隧道的情况下，这需要多身份证书或 RFC 3546 或者其他的协议的配置，但都是为了相同的目的。

UE 和 BSF 将会存储密钥 Ks 和与其相关的 B-TID，直到 Ks 的生存期满，或者密钥 Ks 被更新了，或者删除条件满足时。

注 5：以下情况会出现。UE与NAF1联系并生成密钥。然后，UE与NAF2联系并生成密钥。接着，NAF1向BSF请求密钥，但是旧密钥已经被覆盖了，因为NAF2又进行了新的GBA过程。在联系完NAF1（B-TID1）后，UE又开始了新一轮的GBA过程（B-TID2），并通过Ua口向NAF1发出请求。一个可能是B-TID1的生命周期就要到期了。非常有可能的是：GBA过程花费了太多的时间（由于HSS的介入），B-TID1已经到达了BSF。这种乱续问题非常少见。这种错误情况会返回给UE，B-TID2也会被NAF1使用。乱续情况会自愈，因为如果BSF不能识别B-TID1，那么Ua请求就失败了。UE会使用B-TID2发送一个新的请求。

5.1.5.3 使用建立安全关联的过程

在UE和NAF进行通信之前，UE和NAF首先必须协商是否使用以GBA方式产生的共享密钥。如果UE不知道与NAF是否使用GBA，它就需要使用在前面章节中描述的自举初始化过程。

一旦UE和NAF使用GBA建立了联系，UE与NAF每次交互都需要执行图11描述的几步。

a）UE 通过参考点 Ua 向 NAF 发起通信：

1）一般情况下，UE 和 NAF 还没有共享需要保护参考点 Ua 的密钥。如果已经共享了这个密钥（Ks_NAF 对于相关的密钥衍生参数已经是有效的），UE 和 NAF 就可以立刻进行安全的通信。如果 UE 和 NAF 还没有共享这个密钥，UE 就需要执行以下步骤：

① 如果 UE 对于选择的 UICC 应用的密钥 Ks 是有效的，UE 就可以根据 Ks 衍生出密钥 Ks_NAF。

② 如果 UE 内对于选择的 UICC 应用的密钥 Ks 是无效的，UE 首先要先与 BSF 通过参考点 Ub 协商

标准分享网 www.bzfxw.com 免费下载

一个密钥 Ks，然后进行衍生 Ks_NAF 的过程。

对于UICC应用，如果UE不想根据同一个密钥衍生多个Ks_NAF，UE就应该先与BSF通过参考点Ub协商一个新的密钥Ks，然后进行衍生Ks_NAF的过程。

2）如果 NAF 与 UE 共享一个密钥，但是 NAF 要去更新这个密钥。比如说，这个密钥的生存期满或者马上到期，再或者这个密钥不能满足 NAF 本地有效条件，它就需要发送一个合适的自举重协商请求到 UE。如果密钥的生存期满，运行在上面的协议将会终止。这种通知的方式决定于运行在上面的协议。如果 UE 接收到自举重认证请求，它将会按照 5.1.5.2 节说明的方式执行，目的是获得一个新的密钥 Ks。

考虑到在UE和BSF内衍生密钥的一致性，两者都需要使用相同的FQDN进行衍生。运行在Ua上的协议都需要是指定在下列情况：只有5.1.5.2节的注1和注2被允许用于NAF，或者当Ua口使用的协议从UE到NAF传输用于产生衍生密钥的FQDN时。

注 1：如果在UE和NAF之间的共享密钥无效了，NAF就可以为后来的删除设置相关安全关联的删除条件。

3）UE 以 5.1.3.2 节中描述的方式把 B-TID 发送给 NAF，这样可以使 NAF 从 BSF 内获得相关的密钥。

注 2：UE 可以根据参考点Ua的特殊需要来调整密钥资料Ks_NAF。这种调整超出了本规范的内容。

4）在 ME 里 GBA 相关密钥的密钥管理（即 Ks 和 Ks_NAF）在 5.1.4.11 节描述。

5）当通过参考点 Ub 协商出新的密钥 Ks，NAF_Id 产生的密钥 Ks_NAF 被更新时，存储在 UE 内由与这个 NAF_Id 不同的 NAF_Id 产生的 Ks_NAF 将不会受到影响。

对于每个NAF-Id，UE内至多存储一个与之相对应的Ks_NAF。

b）NAF通过参考点Zn与BSF开始通信，

1）NAF根据通过Ua口UE提供的B-TID请求相应的密钥资料；

2）NAF还可以为应用请求一个或多个特定应用的USS，通过Ua口从UE接收的请求可以接入；

注 3：如果NAF需要服务的连续性，那么NAF可以根据BSF策略请求一个包含用户假名可以允许服务连续性的USS。

3)随着密钥资料请求，NAF应该提供NAF-Id(其包括UE用来接入这个NAF的FQDN和Ua安全协议 标识）给BSF。（这样是为了以下步骤BSF和UE密钥衍生的连续性）。BSF应该能够确认NAF有权使用这个FQDN。

c)BSF 根据密钥 Ks 和密钥衍生参数衍生出密钥，该密钥用于保护参考点 Ua 上使用的协议(在 5.1.3.2 节里有详细说明)。然后将 Ks_NAF，自举时间，密钥的生存期和 GBA 类型发送给 NAF。如果在用户 GUSS 里面存在可以使用的 USS，并且这个 NAF 有权获得所请求的 USS，则 BSF 也将所请求的应用相关的以及潜在的 NAF 组相关的 USS 与 Ks_NAF 一起发送到 NAF。对于任意包含 NAF 组特征的 USS，这个特征应在提供给 NAF 时在 USS 里删除。如果 NAF 所提供的由 B-TID 所标识的密钥在 BSF 里面无效，则在对 NAF 的响应消息里通知 NAF。NAF 将会向 UE 发起一个自举重认证请求。

注 4：NAF可以根据本地策略，来设置Ks_NAF的本地有效条件。比如说，限制Ks_NAF重利用次数。

注 5：NAF将使用与UE同样的方式来调整Ks_NAF去适应参考点Ua的相关要求。该调整超出了本部分的范围。

1）BSF 可能要求在用户的 GUSS 内对应某个 NAF 必须存在的一个或多个与应用相关并且与潜在的 NAF 组相关的 USS。如果 GUSS 缺少一些要求的设置，则 BSF 就需要在向 NAF 响应中指出这一点。

2）BSF 还可能根据 BSF 的策略将私人用户标识（IMPI）和所请求的 USS 发送给 NAF。

d）NAF 通过参考点 Ua 上的协议继续与 UE 进行交互。

一旦运行在参考点 Ua 上的协议完成，就达到了自举的目的，因为这能够使得 UE 和 NAF 在参考点 Ua 上安全的进行通信。

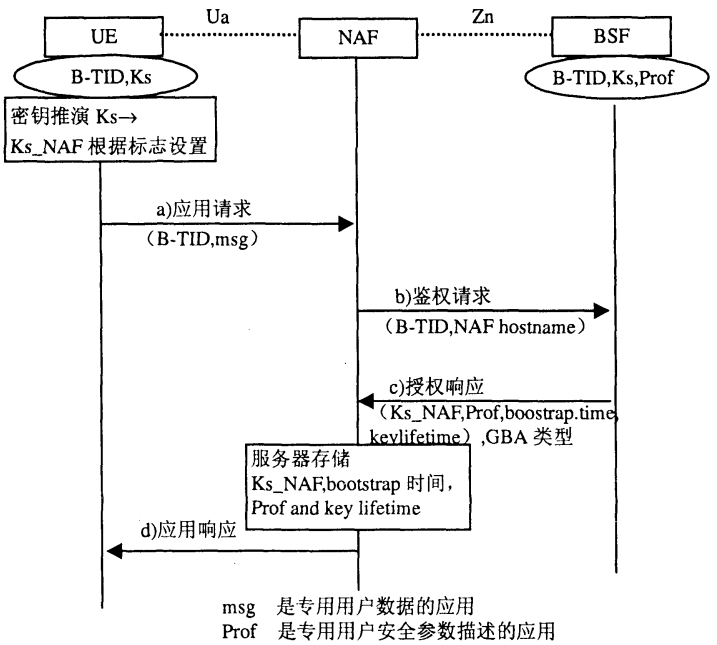


图11 自举应用过程

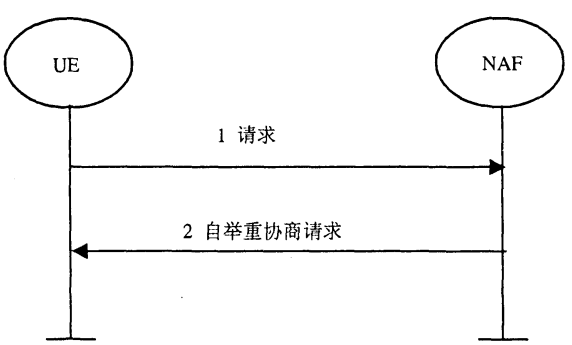


图12 自举重认证请求

5.1.5.4 服务发现过程

UE应该根据在自举过程中使用的UICC应用的身份信息（例如：USIM的IMSI，ISIM的IMPI）按照以下方式来发现BSF的地址。对于在自举中使用USIM的情况，BSF的地址根据TS23.003描述的来衍生。

5.2 UICC 增强型 GBA（GBA_U）

在本节所描述的过程假设UICC，BSF和HSS能够处理GBA_U相关的增强。本节所描述的过程同样适用于NAF不支持GBA_U的情况。

5.2.1 基于 UICC 增强的自举的框架和参考点

本标准的5.1.4节的内容同样适用于此。另外在ME与UICC之间的接口（见TS 31.102和TS 31.103）必须进行增强，以支持GBA_U相关的命令。对这些命令的要求在5.2.2.1中有所描述。细节见5.2.3节中的描述。

基于UICC增强的自举的框架和参考点参见附录K。

5.2.2 基于 UICC 增强的自举的要求和原理

标准分享网 www.bzfxw.com 免费下载

5.1.3节的要求与原则同样适用在这里。除此还要增加以下部分：

5.2.2.1 UE 的要求

运行参考点Ub上的协议所产生的3G AKA密钥CK和IK不能离开UICC。

UICC应该能够区分对于GBA_U的认证请求和其他3G认证域的认证请求。

收到ME的认证请求后，UICC知道这个请求与GBA_U相关，UICC必须衍生出自举密钥。

收到ME的请求后，UICC还必须能利用存储在UICC上的密钥衍生出NAF相关密钥。

所有支持GBA的ME都必须支持前面两种请求的过程。

5.2.2.2 BSF 的要求

BSF应该支持GBA_U和GBA_ME两种自举过程。使用哪一种方式要取决于签约信息（比如说UICC能力）。

BSF应该可以从从HSS中获得的GBA用户安全设置中获知与GBA相关的UICC能力。

5.2.3 基于 UICC 增强的自举过程

5.2.3.1 自举的初始化

5.1.5.1节所述同样适用于此。

5.2.3.2 自举过程

在本节所描述的过程中，对密钥和认证向量在UE和BSF中的处理不同于5.1.5.2中所描述的过程。2个过程通过参考点Ub交换的信息都是相同的。

当一个UE要与NAF进行交互，并且知道需要自举过程，则UE将（必须）首先执行这个自举认证（图13）。否则，只有当UE接收到从NAF发来的自举请求消息或者自举重认证消息，或者UE内的密钥到期时，UE才会执行自举认证（见5.2.3.3）。

注：为了便于阅读，TS 33.102中AKA协议的规范和RFC 3310中HTTP摘要AKA协议的规范的主要步骤在图13中进行了重复说明。在任何潜在冲突的情况下，TS 33.102和RFC 3310的规范都具有优先权。

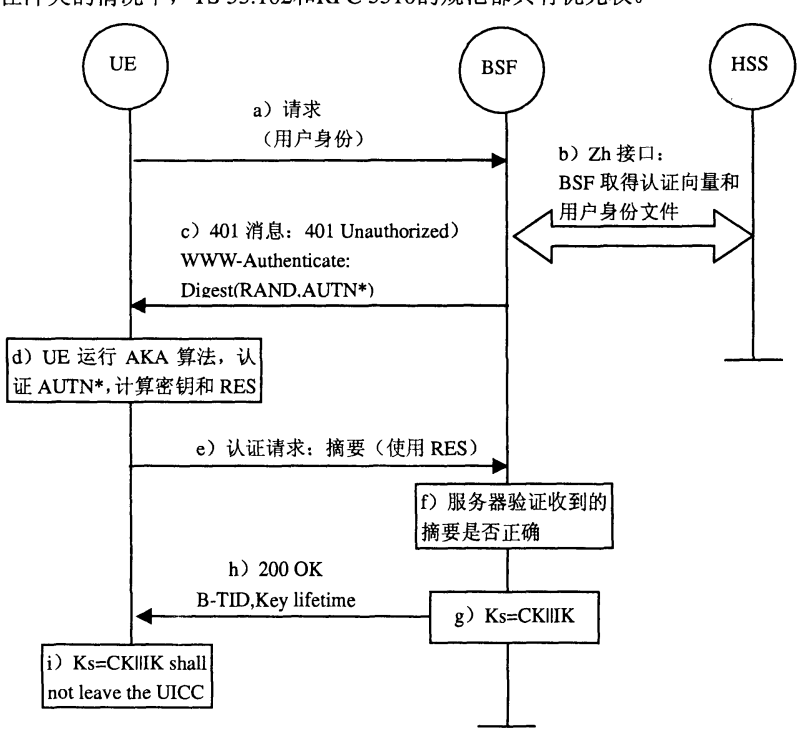


图13 基于 UICC 增强的自举过程

a）ME向BSF发送HTTP请求，包括用户的身份信息B-TID，如果没有有效的B-TID，则发送IMPI。

b）BSF通过参考点Zh从HSS获得GBA用户安全设置和一组认证向量（AV，AV=RAND||AUTN||XRES||CK||IK）。

如果BSF在上一次自举过程应用时间戳选项，并且有从HSS得到的签约用户的本地GUSS的拷贝，这个GUSS包括时间戳，那么BSF可以在请求信息里包括GUSS时间戳。得到时间戳后，如果HSS应用时间戳选项，那么HSS将它与储存在HSS里的GUSS时间戳比较。在这种情况下，当且仅当HSS作了比较并且时间戳相等时，HSS将“GUSS时间戳相等”指示发送给BSF。在其他情况下，HSS把GUSS（如果存在）发送给BSF。如果BSF接收到“GUSS时间戳相等”指示，它就存储GUSS的本地拷贝。其他情况，BSF删除GUSS的本地拷贝，并且存储得到的GUSS（如果发送）。

然后BSF根据USS，决定使用GBA_U。这种情况下，BSF按下面方法进行：

BSF计算MAC * = MAC⊕Trunc（SHA-1（IK））

注1：Trunc指在FIPS PUB 180-2（2002）：“安全Hash标准”所输出的160比特中的[0]到[63]比特用在MAC的*操作中。BSF在去掉最低有效位后，存储XRES。

注 2：在多个HSS环境中，优先于步骤2，BSF可以通过询问SLF得到储存用户签约的HSS地址。

c）BSF将RAND和AUTN *（AUTN * = SQN⊕AK ‖ AMF ‖ MAC *）以401的消息方式发送给UE。这是要求UE去认证BSF。

d)ME将RAND和AUTN * 发送到UICC。UICC计算IK和MAC(MAC= MAC * ⊕Trunc(SHA-1(IK)))。然后UICC通过验证AUTN（比如：SQN⊕AK ‖ AMF ‖ MAC）去证明该挑战来自于授权网络。UICC也计算出CK和RES。这将会在BSF和UICC内产生会话密钥CK和IK。UICC然后把RES传输到ME（去掉最低有效位后），并且保存Ks，该Ks是UICC中的CK和IK的串接后的结果。

e）ME发送另外一个HTTP请求到BSF，请求中包含摘要AKA响应（利用RES计算出来的）。

f）BSF根据摘要AKA响应认证ME。

注 3：在“AKAv1”中的HTTP摘要AKA的密码是二进制。

g）BSF通过连接CK和IK来产生密钥资料Ks。通过对步骤3里的RAND值进行base64编码，并与BSF服务器名共同编码，以NAI的格式来产生B-TID值，即，base64encode（RAND）@BSF_servers_domain_name。

h）BSF将（必须）向UE发送200 OK消息以向其指示本认证的成功。消息中包含B-TID。除此之外，在这个200 OK消息中还要包含这个密钥Ks的有效期。

注： 如果步骤1采用用户身份标识B-TID，则步骤8中BSF发送给UE的B-TID需要加密发送。

i）UICC和BSF将（必须）会在5.2.3.3节中描述的过程中使用Ks来衍生出NAF相关密钥Ks_ext_NAF和Ks_int_NAF。Ks_ext_NAF和Ks_int_NAF是用来保护参考点Ua上的安全。

Ks_ext_NAF在UICC里面以这个公式来计算的：Ks_ext_NAF = KDF（Ks，“gba-me”，RAND，IMPI，NAF_Id）；Ks_int_NAF在UICC里面以这个公式来计算的：Ks_int_NAF=KDF（Ks，“gba-u”，RAND，IMPI，NAF_Id），在这里KDF是在附录A里面说明的密钥衍生函数，密钥衍生参数包括用户的IMPI，NAF_ID和RAND。NAF_ID的结构是：NAF_Id=NAF的FQDN||Ua安全协议标识。Ks_ext_NAF衍生所需的密钥衍生参数应该与Ks_int_NAF所需的衍生参数不同。这通过添加一个静态字符串来完成，在

标准分享网 www.bzfxw.com 免费下载

Ks_ext_NAF衍生函数中添加“gba-me”作为输入参数，在Ks_int_NAF衍生函数里添加“gba-u”作为输入参数。

注 4：如果一个NAF拥有有相同FQDN和Ua安全协议标识的2个或多个应用，那么它们应共享相同的NAF衍生密钥。这会引起所谓的“two-time pad”，会导致这些应用的安全妥协的情况。这可以通过分别进行自举过程或者应用的特定方法避免，这超出了本标准范围。

在UE和BSF里，为了允许基于NAF名的密钥衍生连续性，5.1.5.2节描述的前提条件至少有一个要满足。

UE 和 BSF 将会存储密钥 Ks 和与其相关的 B-TID，直到 Ks 的生存期满，或者密钥 Ks 被更新了，或者删除条件满足时。

5.2.3.3 使用建立安全关联的过程

在UE和NAF进行通信之前，UE和NAF首先要协商它们之间是否需要使用GBA方式获得的共享密钥。如果UE不知道与NAF是否使用GBA，则它将使用5.2.3.1节中描述的自举过程的触发过程。

UE和NAF一旦协商好采用GBA，则UE每次和NAF交互都要执行图14所描述的步骤。

接下来，UE和NAF需要协商使用哪种类型的密钥，Ks_ext_NAF或者Ks_int_NAF，或者两种都使用。缺省时只使用Ks_ext_NAF。MEs和不支持GBA_U的NAFs也支持这种使用方式。如果Ks_int_NAF，或者Ks_ext_NAF和Ks_int_NAF被使用，UE和NAF必须在执行5.2.3.3后面的部分所描述的过程之前，协商好使用哪种密钥。任何的协商都可代替默认的使用方式。密钥选择指示，即NAF在Ua口使用哪一种密钥（即Ks_ext_NAF或Ks_int_NAF），根据定义在stage 3的规范可以包含在应用特定USS里。如果指示存在，NAF使用指示的密钥。如果USS里指示的是Ks_int_NAF，那么UE想要使用Ks_ext_NAF，则NAF应该终止与UE的通信。

注 1：这个协商过程可以由定义UE和NAF之间参考点Ua的规范来规定，比如：在TS 33.246规范中对MBMS中的使用GBA的规定，这个协商也可以由NAF和UE通过参考点Ua协商决定，或者通过配置来完成。

a）UE可以利用密钥Ks_ext_NAF或者Ks_int_NAF，再或者两者，通过参考点Ua与NAF进行通信。过程如下：

— 一般来说，UE和NAF没有共享用来保护参考点Ua的共享密钥。如果真的不存在，UE就需要执行以下过程：

1）如果需要 Ks_ext_NAF，并且 UICC 中对于选定的 UICC 应用存在一个有效的密钥 Ks，则 ME 将按照 5.2.3.2 节中描述的过程来请求 UICC 利用 Ks 衍生出密钥 Ks_ext_NAF。

2）如果需要 Ks_int_NAF，并且 UICC 中对于选定的 UICC 应用存在一个有效的密钥 Ks，则 ME 按照 5.2.3.2 节中描述的过程来请求 UICC 利用 Ks 衍生出密钥 Ks_int_NAF。

对于选定的UICC应用，如果UE不希望使用相同的密钥Ks产生多个Ks_ext/int_NAF，则UE首先需根据5.2.3.2节描述的过程，通过参考点Ub与BSF产生新的密钥Ks，然后衍生出所需的Ks_ext_NAF 或者Ks_int_NAF，或者两者。

3）如果对于选定的 UICC 应用，在 UE 内没有有效的密钥 Ks，则 UE 首先需根据 5.2.3.2 节描述的过程，通过参考点 Ub 与 BSF 产生新的密钥 Ks，然后衍生出所需的 Ks_ext_NAF 或者 Ks_int_NAF，或者两者。

4）如果 NAF 与 UE 已经共享一个密钥，但是 NAF 需要对这个密钥进行更新，则 NAF 向 UE 发送

一个合适的自举重认证请求。如果密钥的有效期满，则运行在参考点 Ua 上的协议也将终止。这个指示的格式取决于使用在参考点 Ua 上的具体的协议。如果 UE 接收到一个自举重认证请求，则 UE 将会根据 5.2.3.2 节中描述的过程来运行 Ub 上的协议，以获得新的密钥。

注 2：如果在UE和NAF之间的共享密钥变的无效，则NAF将可以对相应的安全关联设置为删除状态，以便于后面进行删除。

注 3：如果NAF要求不能使用同一个Ks衍生多个Ks_int/ext_NAF，则NAF在对UE的第一个请求的响应中，就要给UE发送密钥更新请求。

5）UE 根据 5.2.3.2 节描述的方式将 B-TID 发送到 NAF，NAF 根据 B-TID 从 BSF 中获得相关的密钥。

为了保持UE和BSF一致的密钥衍生，它们在密钥衍生时要使用同样的FQDN（见5.1.5.2节的注2）。运行在Ua上的每个协议都应该规定是否只允许NAF具有5.1.5.2节中注2的前两种情况，或者运行在Ua上协议是否向NAF传送UE衍生密钥时所用的FQDN。

注 4：UE应该调整Ks_ext_NAF或者Ks_int_NAF去适应参考点Ua上的相关需要。如何调整超出了本规范的范围。

6）ME 中与 GBA 相关的密钥管理（例如 Ks_ext_NAF）描述在 5.1.4.11 节：

— UICC 中所有 GBA 相关密钥在 ME 关机时没有必要删除。

注 5：每次参考点Ub上的协议运行完成以后，根据5.2.3.2节的步骤在UE内将会产生一个新的Ks和一个新的Ks相对应的B-TID，以至于UE内不可能同时存在不同的B-TID的密钥Ks。

7）当通过参考点 Ub 协商出一个新的密钥 Ks，并且需要对一个 NAF_Id 衍生出新的 NAF 相关密钥时，那么与 NAF_Id 对应的 Ks_ext_NAF 和 Ks_int_NAF 也要进行更新，但是存储在 UE 内与其他 NAF_Id 相关的 Ks_ext_NAF 和 Ks_int_NAF，不会受到影响。

根据5.2.3.2节和5.2.3.3节描述的过程，UE内对于每个NAF_Id至多存储一个Ks_int_NAF/Ks_ext_NAF密钥对。

注 6：这个规则保证了UE和NAF内Ks_ext_NAF 和Ks_int_NAF的同步。

b）NAF 通过参考点 Zn 与 BSF 进行通信。

1）NAF 向 BSF 请求与 B-TID 相关的密钥，这个 B-TID 是 UE 通过参考点 Ua 发送给 NAF 的。如果 NAF 可执行 GBA_U，那么它在请求消息中包含一个相应的标志来进行指示。

注 7：如果NAF要求服务连续性，那么NAF可以根据BSF策略请求一个包含用户假名可以允许服务连续性的USS。

2）对于 UE 通过参考点 Ua 可能接入的应用，NAF 可以请求一个或者多个与该应用相关 USS。

3）通过 Zn 口的密钥请求，NAF 应该向 BSF 提供 NAF-Id（其包括 UE 用来接入这个 NAF 的 FQDN 和 Ua 安全协议标识）。（这样是为了以下步骤 BSF 和 UE 密钥衍生的连续性）。BSF 应该能够确认 NAF 有权使用 FQDN。

c）BSF 根据 5.2.3.2 节描述的过程衍生出 Ks_ext_NAF 和 Ks_int_NAF（如果需要）。如果 NAF 在请求中告知 BSF 其支持 GBA_U，则 BSF 向 NAF 提供两个密钥，Ks_ext_NAF 和 Ks_int_NAF，否则 BSF 只提供 Ks_ext_NAF。另外，BSF 还提供自举时间，这些密钥的生存期，GBA 类型。如果在用户 GUSS 里面存在可以使用的 USS，并且这个 NAF 有权获得所请求的 USS，则 BSF 也将所请求的应用相关的并且与潜在的 NAF 组相关 USS 发送到 NAF。对于任意包含 NAF 组特征的 USS，这个特征应在提供给 NAF 时在 USS 里删除。如果 NAF 所提供的由 B-TID 标识的密钥在 BSF 里面无效，则将此无效信息在响应中返回 NAF。NAF 将会向 UE 发起一个自举重认证请求（参看图 12）。

标准分享网 www.bzfxw.com 免费下载

注 8：NAF根据本地策略来设置Ks_NAF的本地有效条件，比如说Ks_NAF的重利用的限制次数。

注 9：NAF使用与UE同样的方式来调整Ks_ext_NAF和Ks_int_NAF，以适应参考点Ua的相关需要。如何调整超出了本规范的范围。

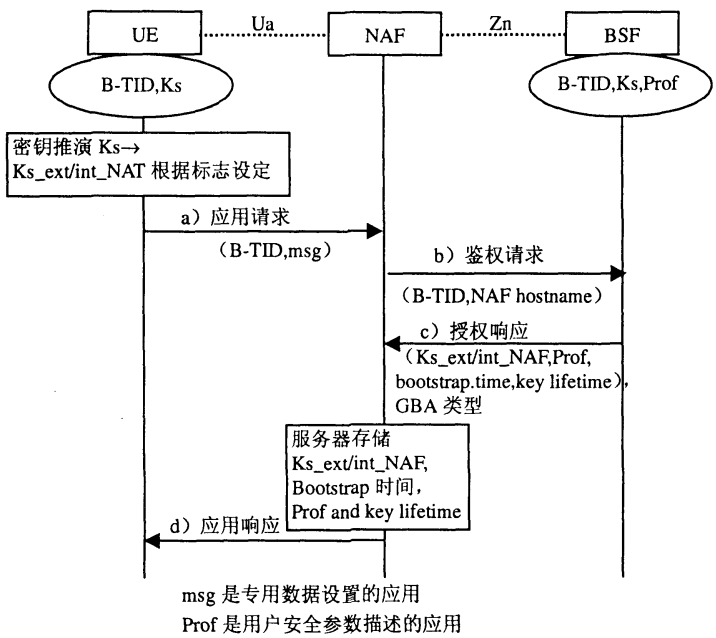


图14　基于 UICC 增强的自举使用过程

1）BSF 可以要求 GUSS 内应该存在针对某个 NAF 的一个或多个与应用相关并与潜在的 NAF 组相关的 USS（参看 5.1.4.6 节）。如果 GUSS 缺少一些要求的设置，则 BSF 就需要在向 NAF 回复中显示出这一点。

2）BSF 根据 BSF 的策略还可能将私人用户标识（IMPI）和所请求的 USS 发送给 NAF。

d）NAF 通过参考点 Ua 上的协议继续与 UE 进行交互。

——如果 NAF 从 BSF 请求一个特定应用的 USS，并且这个 USS 回到了 NAF，那么 NAF 应该检查是否这个 USS 包含密钥选择指示。如果存在密钥选择指示，NAF 只使用指示的密钥。如果 Ua 口使用了一个不同的密钥，那么在 Ua 口上的协议应该终止。

一旦运行在参考点 Ua 上的协议完成，就实现了自举的目的，就是使得 UE 和 NAF 之间可以在参考点 Ua 上安全的进行通信。

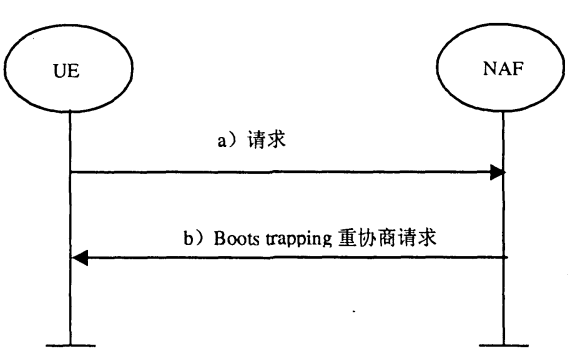


图15　自举重认证请求

5.2.3.4　服务发现过程

本文档中5.1.5.4节的内容在这里同样适用。

5.3 终端分离情况下的增强通用认证框架

5.3.1 参考模型

图16显示了NAF应用客户端和GBA客户端分离状态下的增强GAA框架示意图。

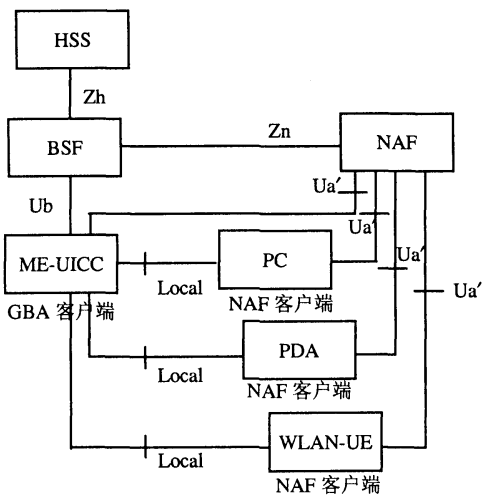


图16 NAF 应用客户端和 GBA 客户端分离状态下的增强 GAA 框架示意

随着很多GAA应用范围越来越广泛，出现一些新的应用场景。其中一个比较大的应用场景就是终端分离的情况，所谓终端分离情况，就是某个移动用户具备多个终端设备，除了手机以外，还具备其他终端设备如PC机，WLAN-UE，掌上电脑等，而这些终端通过同一个（U）SIM卡用户信息访问网络业务，如图16所示，导致NAF应用客户端和UE不在同一个设备上。如图16所示这种情况下的GAA架构，可以称为增强GAA框架，这种情况下NAF应用客户端不在UE上，而是在UE以外的某一个或者某几个外围终端设备上。当这些外围终端设备不具备（U）SIM或者不使用自身的（U）SIM时，就会出现NAF应用客户端在外围终端设备上，与执行GBA的客户端不在同一个设备上的情况。现有的GBA架构主要针对NAF应用客户端与GBA客户端在同一个终端的情况，尚没有针对图16所述GAA构架方式的认证方法。

当多个外围终端设备共享一个UE上的GBA客户端时，如果这些外围终端设备中的某两个或者某几个访问同一个NAF时，还会出现多个外围终端设备采用同一个衍生密钥与某一个NAF通信的情况，存在安全隐患，即一个设备泄漏了密钥会影响到其他与之使用相同密钥的设备。

这就需要有一种安全机制来解决以上的问题。附录K提供了3种解决方案供参考。具体见附录K。

6 用户证书的支持

本章描述了通过第5章所描述的机制分发用户证书的过程。用户证书支持运营商协助提供和直接提供的业务。

本部分呈现了向用户分发证书的信令流程，证书和数字签名的格式。本文不欲重复相同主题的已有标准，将尽可能引用已有的适用规范。

6.1.1 介绍

数字签名可用于例如移动商务，业务授权和计费的安全保证。但是只有数字签名还不够，进一步的需求要求对业务授权和计费的全局支持。本规范规定了，用于保证移动网业务授权和计费全局安全的基础设施，来支持局部的数字签名体系。

标准分享网 www.bzfxw.com 免费下载

利用本部分所述机制分发的用户证书提供了进一步实现全局公钥基础设施（PKI）的途径。局部的数字签名体系是可扩建的；一个运营商可以建设独立于其他运营商的建设局部的数字签名体系。另一方面，用户和服务运营商对数字证书的使用有利于全局公钥基础设施（PKI）的建设。

3GPP系统应能在归属网和访问网分发用户证书来进行业务使用的授权和计费。这就需要以下规范：

a）为用户发放临时或长期证书的流程

b）证书和数字签名的标准格式，例如引用OMA无线PKI规范。

此机制应允许采用经济有效的方式实现UE的安全能力。此机制应允许用户在调用业务的同时可被网络识别，但对业务提供商可匿名。

OMA提供了另一种证书登记的方案（参见6.1.5节）。

用户证书支持运营商协助提供的业务和运营商直接提供的业务。本部分不需要对那些业务加以标准化。服务提供商和运营商之间的通信（以证书发放者的角色）也不需在本部分中讨论。

6.1.2 参考模型

图17展示了网络模型简图，包括证书发放相关的网络实体及连接它们的参考点。

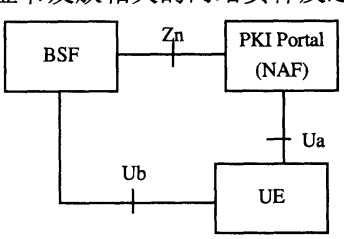


图17 证书发放的网络模型简图

6.1.3 网元

6.1.3.1 PKI 入口

一个PKI应发放UE证书和传递运营商CA证书。在这2种情况下，用事先已在UE和BSF间建立的密钥材料来保护请求和响应消息。

在PKI术语中，PKI入口就是RA（Registration Authority），根据用户的签约用来认证证书请求。PKI入口也可以作为颁发证书的CA（Certification Authority）。但是也可以在已经存在的PKI基础设施中发放证书，PKI入口只作为RA，而CA在PKI基础设施中。

6.1.3.2 自举服务器功能

自举服务功能（BSF）应能通过提供认证和PKI入口特定的用户安全设置（即，用户是否能注册某种用户证书）来支持PKI入口的功能。

6.1.3.3 用户设备（UE）

对UE的新功能要求是支持参考点Ua（证书登陆协议），Ua受共享密钥保护，共享密钥由自举功能建立。

此外，UE可能有能力产生公私钥对，有能力将私钥部分保存在非易失寄存器中（例如在UICC）和保护私钥部分的使用（例如用PIN）。

6.1.4 发放用户证书的需求和原则

发放用户证书有以下前提：

1）UE和移动运营商PKI入口共享密钥材料来支持证书请求和运营商CA证书恢复。

2）根据用户归属PKI入口的特定用户安全设置来发放被请求的证书。PKI在发放用户证书前负责查实。

当私有密钥存于WIMOMA：“无线身份模块；安全”时，应可能将此信息和证书请求一同发送。WIM能证明密钥的来源（确保密钥安全地保存于一个防篡改的设备）。

注：保证密钥来源的方法不仅限于使用 WIM。

6.1.4.1 自举的使用

用户证书和运营商CA证书的分发流程所用的之共享密钥应基于3GPP通用自举架构，详见第5章。

6.1.4.2 接入独立

用户证书和运营商CA证书发放流程不依赖于接入方式。证书发放流程需要有与UE的IP连接。

6.1.4.3 漫游和业务网的支持

漫游用户应可以从归属网络请求用户证书和运营商CA证书。

漫游用户应可以从拜访网络请求用户证书和运营商CA证书。归属网应能控制是否允许拜访网络给漫游用户发放用户证书（见6.1.4.4节）。

6.1.4.4 归属运营商的控制

归属运营商应能控制用户证书的分发。控制包括允许发放给谁和证书的类型。

运营商的控制需要GBA用户安全设置信息的支持。对于应每种用户证书，即对于WAP证书和CRL档案OMA：“WAP证书和CRL描述”中不同的密钥用法，用户的PKI入口特定的安全设置应包含一个标志来允许或不允许发放这种证书发放给用户。根据WAP证书和CRL档案OMA：“WAP证书和CRL描述”，有两种用户证书：用于认证的用户证书和用于数字签名的用户证书（即抗抵赖）。

运营商CA证书的传送总是被允许的。

6.1.4.5 计费原则

运营商应能对发放用户证书发放或发送运营商CA证书进行计费。

6.1.4.6 用户证书档案

用户证书档案应基于WAP证书和CRL档案OMA：“WAP证书和CRL描述”，WAP证书和CRL档案则基于IETF RFC 3280和ITU-T X.509。一个证书档案定义了特定的上下文中证书的格式和语义。WAP证书和CRL档案OMA：“WAP证书和CRL描述”规范定义了4种证书档案：两种用户证书档案，一种是用于认证，另一种是用于抗抵赖，用于针对认证的服务器证书档案，和授权证书档案（即CA证书）。由于用户证书发放给用户并且由于业务需要CA证书来验证用户证书和用户证书档案一起使用的相关的WAP证书档案就是用户证书档案，和CA证书档案。

如果发放证书的运营商采用的证书处理方法满足文献中的要求，合格的IETF RFC 3039和ETSI TS 101 862证书档案也可以用作用户证书档案。

在证书请求中，下列证书扩展可以填充UE提供的信息：

证书用途（即用keyUsage和/或extKeyUsage扩展OMA：“WAP证书和CRL描述”）。

用户标识（即subject name域和可能在subjectAltName扩展中定义的额外标识OMA：“WAP证书和CRL描述”）。运营商CA应对每个提议的用户标识加以授权。

——密钥来源证明（即keyGenAssertion）。运营商CA应验证密钥来源证明。

注：不强制运营商 CA 将 UE 提议的扩展加入到证书中。运营商 CA 应根据自己的证书策略来分发证书。可以制定证书实践声明（CPS）来描述一般的需求和证书分发的步骤。

6.1.4.7 业务发现

标准分享网 www.bzfxw.com 免费下载

为了进行证书登陆流程，宜在UE中配置自举服务器和PKI入口的地址。第5章中定义了发现BSF发现的方法。

需要规定如何发现PKI入口的地址的流程。应可以通过以下方式对UE进行手工或自动配置：

1）应通过可靠的渠道发布地址信息。用户应储存所有的参数作为建立 IP 连接建立的一部分。地址信息只需输入一次。

2）在自举业务定购被接受时，地址信息应以 OTA 的方式被自动推送到 UE 中。所有的参数应在 UE 中存储，使用方式同上。详细流程的定义在 OMA“Provisioning Content Version 1.1”。

6.1.4.8 对 Ua 参考点的要求

1）UE 应能从 PKI 入口请求用户证书，PKI 在网络连接中扮演 NAF 角色；

2）NAF 应能认证 UE 的证书请求；

3）UE 应能通过网络连接获取运营商的 CA 证书；

4）UE 应能认证 NAF 响应（即，运营商 CA 证书的传递）；

5）此流程应独立于所使用的接入网络；

6）NAF 应有权接入到用户 PKI 入口特定的用户安全设置来检查证书策略。这意味着参考点 Zn 应支持获取 GBA 用户安全设置的部分信息；

7）到 UE 的证书响应和传送应在初始证书请求的几秒内完成；

8）证书请求格式应是 PKCS#10 IETF RFC 2510；

9）证书响应格式应是以下之一：证书，指向证书的指针，或完整的证书链。

6.1.5 证书发放架构

6.1.5.1 参考点 Ua

6.1.5.1.1 概述

在证书发放过程中，参考点Ua用于：

1）运营商 CA 以证书的格式验证用户的公钥；

2）把运营商 CA 证书发送给 UE。

在用户证书的发放过程中，UE 可能会请求一个公钥证书。可以接受的请求格式应是 PKCS#10 IETF RFC 2510，用来封装公钥和其他属性（即用户名、密钥用途，等等）。这一请求从 UE 通过参考点 Ua 传送到 PKI 入口。接收到证书请求之后，PKI 入口将根据自己的证书操作策略和用户 PKI 入口的特定用户安全设置来验证公钥，这一设置是通过 BSF 从 HSS 得到的。如果 PKI 入口决定验证该公钥，它将对其进行数字签名，并生成相应的证书，该证书通过参考点 Ua 从 PKI 入口传回 UE。

在运营商 CA 证书的发送过程中，UE 可能会请求 PKI 入口发送运营商 CA 的证书。在相应的响应中，PKI 入口将把 CA 的证书发送给 UE。由于运营商的 CA 证书是一种典型的自我签名的证书，并且这个 CA 所签名的证书的有效性基于该特定 CA 的证书，所以该运营商的 CA 证书需要通过经过认证的、安全的通道发送。

根据第 5 章中定义的 GBA，对通过参考点 Ua 传送的信息的认证、完整性保护以及可能进行的加密是基于 BSF 生成的共享秘钥，PKI 入口的作用相当于 NAF。

6.1.5.1.2 功能和协议

6.1.5.1.2.1 具有 HTTP 摘要认证（HTTP Digest Authentication）的 PKCS#10

基于PKCS#10 IETF RFC 2510 的证书请求通过使用HTTP请求传往PKI入口，该请求应通过TS 24.109的第5.2条所定义的HTTP Digest Authentication来进行认证和完整性保护。

注：第七章所定义的PSK TLS是另外一种认证和保护证书登录的方法。需要进一步研究是否适宜用该方法取代HTTP Digest Authentication。另外，注意在第7章中是否使用的PSK TLS在Release 6中尚无定论。

通过使用HTTP响应来进行发送证书，可以通过HTTP Digest Authentication来进行认证和完整性保护。HTTP响应的内容类型取决于响应的格式。按照WPKIOMA：“无线应用描述；公钥基础设施定义”中的定义，如果返回的是证书，类型就是“application/x-x509-user-cert”。如果返回的是证书指针，类型就是“application/vnd.wap.cert-response”。按照IETF RFC 3546中的定义，如果返回的是证书链，类型就是“application/pkix-pkipath”。

UE在URI请求中发送具有特定参数的明文的HTTP GET请求来要求发送CA证书。该请求可以通过HTTP Digest Authentication来进行认证和完整性保护。

通过使用HTTP响应来发送CA证书，应通过HTTP Digest Authentication对该响应进行认证和完整性保护。HTTP响应的内容类型应是“application/x-x509-ca-cert”。注意当某个新的CA证书付诸使用时，宜随时通知用户。

6.1.5.1.2.2 密钥生成

如果私钥存储于UICC（例如在WIMOMA：“无线应用描述；公钥基础设施定义”中），并且UICC需要特殊的授权（例如来自运营商）来产生密钥，那么移动设备可能需要向NAF发送一个HTTP请求，可能通过HTTP Digest Authentication对该请求进行认证和完整性保护。发送请求的目的是为了发送由UICC产生的nonce。这将允许NAF直接认证UICC应用，并且提供密钥生成所需的授权。确切的密钥生成过程在OMA的“Crypto Object for the ECMAScript Mobile Profile”OMA：“ECMAScript移动文件的密码对象”中有详细定义。

6.1.6 证书发放过程

6.1.6.1 证书发放

a）初始的 HTTP 请求；

b）带有认证质询的 HTTP 响应；

c）UE 得到由 WIM 计算出的 GetKeyAssurance，并且计算 HTTP Digest 的值；

d）带有认证质询响应和 WIM 质询请求的 HTTP 请求；

e）PKI 入口取回基于用户名的会话密钥，并且检验“授权”头，如果成功，它将处理 WIM 质询；

f）带有 WIM 质询响应的 HTTP 响应；

g）UE 产生 PKCS#10 请求；

h）带有 PKCS#10 的 HTTP 请求；

i）PKI 入口处理 PKCS#10 请求；

j）带有用户证书的 HTTP 响应；

k）UE 把证书存储在证书库中。

上面的流程图描述了使用带有 HTTP Digest authentication 的 PKCS#10 时的证书请求。如果 UE 中没有 WIM 应用，那么 c）~e）步骤中涉及 WIM 应用的操作应被忽略。该过程得到安全保护，如 TS 24.109 的第 5.2 条所述。对消息的详细定义留在设备规范中实现。

标准分享网 www.bzfxw.com 免费下载

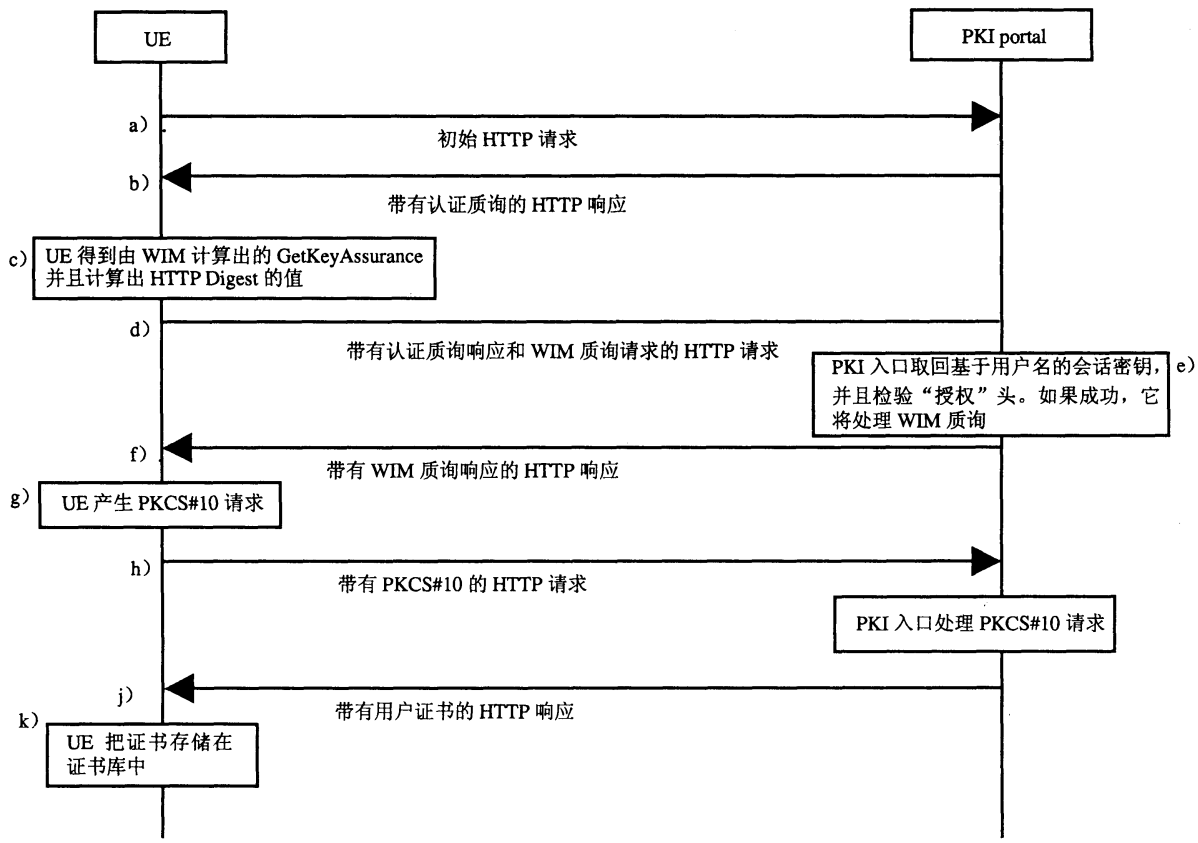


图18 使用具有 HTTP 摘要认证（HTTP Digest Authentication）的 PKCS#10 的证书请求

a）初始的消息是，UE 把一个空的 HTTP 请求发送到 PKI 入口。

b）PKI 入口的响应是 HTTP 代码 401“未授权”，该代码中包含一个 WWW-Authenticate 头。该头指示 UE 使用 HTTP Digest authentication。

c）UE 使用从 BSF 收到的 B-TID 作为用户名和 NAF 特定的会话密钥 Ks_NAF 来计算 Authorization 头的值，生成 HTTP 请求。如果证书请求需要通过 WIM 应用对密钥的来源加以额外的保证，UE 将生成一个 WIM 质询请求，该请求中包含生成密钥来源保证所需要的参数。

d）UE 把 HTTP 请求发送给 PKI 入口，并把 WIM 质询请求放在该请求中。

e)充当NAF角色的PKI入口接收到请求后，将使用B TID从BSF获取NAF特定的会话密钥Ks_NAF，然后使用 Ks_NAF 计算出相应的 digest 值，最后把计算出的值与 Authorization 头中的值相比较，从而验证 Authorization 头。如果验证成功，并且需要 WIM 应用的额外保证，PKI 入口可以使用 PKI 入口特定的用户安全设置来计算 WIM 质询响应。

f）PKI 入口 s 发送回 WIM 质询响应，带有生成后续的 PKCS#10 请求所需的附加参数。PKI 入口可以使用会话密钥 Ks_NAF 来对该响应进行完整性保护和认证。

g）UE 将生成 PKCS#10 请求，并使用 HTTP Digest 请求将其发送给 PKI 入口。如果私钥存储在 WIM 应用中，ME 宜向 WIM 应用请求 AssuranceInfo，并将其放入 PKCS#10 请求中（如果 WIM 应用提供）。登记请求将遵循中所定义的 PKCS #10 证书登记格式。在 OMA ECMA Script 规范中定义了在请求中加入 AssuranceInfo。AssuranceInfo 为处理密钥提供了来源证明（比如，识别 WIM 应用，并且提供密钥存储在该应用中的证明）。UE 可以指示所想要的证书响应格式：证书、证书指针（比如 URL），或者完整的证书链（即从所发放的证书到相应的根证书）。

h）登记请求的格式应如下：

POST <base URL>?response=<indication>[other URL parameters] HTTP/1.1

Content-Type：application/x-pkcs10

<base64 encoded PKCS#10 blob>

其中，

<base URL> 标示一个服务器或程序

<indication> 用来向 PKI 入口指出 UE 所想要的响应类型。可能的值有："single"，仅仅是用户证书；的"pointer"，指向用户证书的指针；或者"chian"，完整的证书链。

[其他 URL 参数]是附加的、可选的 URL 参数。

i）接收到的 PKCS#10 请求将被进一步处理。如果 PKI 入口实际上是一个 RA，PKCS#10 请求将通过任何可用的协议（例如，IETF RFC 2797 中所定义的 CMC 或者 IETF RFC 2510 和 IETF RFC 2511 中所定义的 CMP）转发到 CA。在 PKCS#10 请求得到处理，并且生成证书后，新的证书将被传送回 PKI 入口。PKI 入口将生成一个 HTTP 响应，其中包括证书，或者 WPKI 的 7.4 条所定义的证书指针，或者一个完整的从已发放的证书到根证书的证书链。

j）如果 HTTP 响应包含用户证书自身，它应进行 base64 编码，可以以如下格式分界：

HTTP/1.1 200 OK

Content-Type：application/x-x509-user-cert

-----BEGIN CERTIFICATE-----

<base64 encoded X.509 certificate blob>

-----END CERTIFICATE-----

如果 HTTP 响应包含证书指针，应使用 OMA WPKI 第 7.3.5 条所定义的 CertResponse 结构，可以以如下格式分界：

HTTP/1.1 200 OK

Content-Type：application/vnd.wap.cert-response

-----BEGIN CERTIFICATE RESPONSE-----

<base64 encoded CertResponse structure blob>

-----END CERTIFICATE RESPONSE-----

如果 HTTP 响应包含一个中所定义的 PkiPath 中的完整的证书链，它应进行 base64 编码：

HTTP/1.1 200 OK

Content-Type：application/pkix-pkipath

<base64 encoded PkiPath blob>

证书链的内容类型字段值是"application/pkix-pkipath"，如中所示。

如果证书或者证书指针被发送到 UE，PKI 入口可以使用会话密钥 Ks_NAF 来对响应进行完整性保护和认证。如果完整的证书链被发送到 UE，PKI 入口应对响应进行完整性保护和认证。

k）当 UE 接收到用户证书或者用户证书的 URL 时，将其存储到本地的证书管理系统。

注： On board密钥生成已经在OMA发布的WIM 规范中作了规定。

6.1.6.2 CA 证书发放

标准分享网 www.bzfxw.com 免费下载

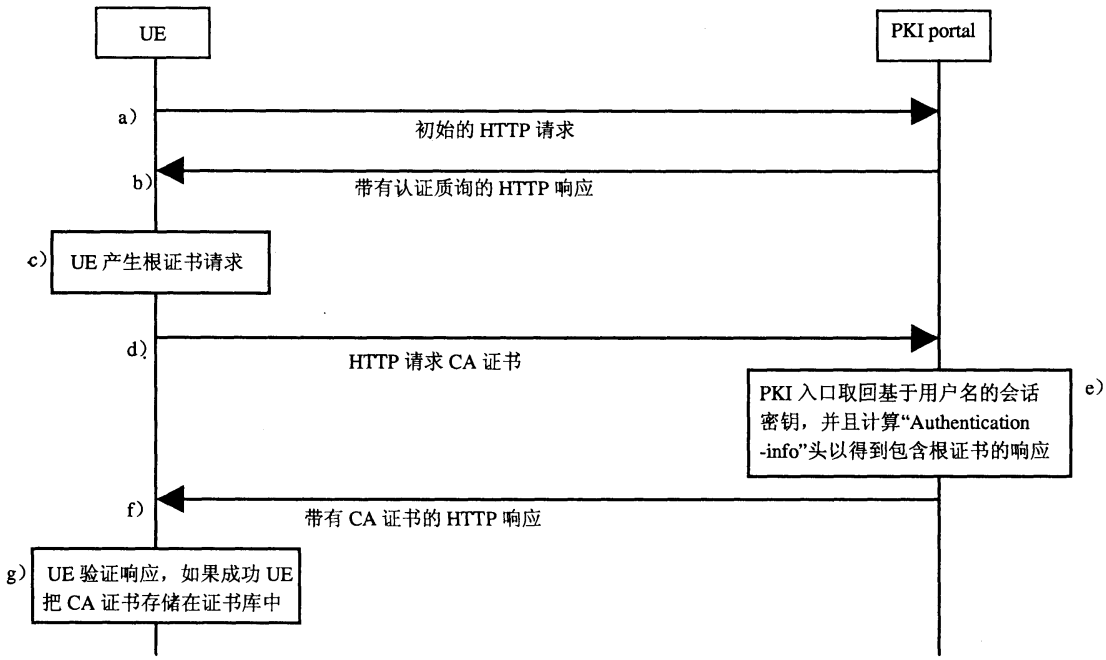


图19　包含 HTTP Digest Authentication 的 CA 证书发送

a）初始的 HTTP 请求；

b）带有认证质询的 HTTP 响应；

c）UE 产生根证书请求；

d）HTTP 请求 CA 证书；

e）PKI 入口取回基于用户名的会话密钥，并且计算"Authentication-info"头以得到包含根证书的响应；

f）带有 CA 证书的 HTTP 响应；

g）UE 验证响应，如果成功，UE 把 CA 证书存储在证书库中。

上面的序列图描述了使用 HTTP Digest authentication 时的 CA 证书发送。该过程得到安全保护，如 TS 24.109 的第 5.2 节所述。对消息的详细定义留在第 3 阶段的规范中实现。

a）初始的消息是，UE 把一个空的 HTTP 请求发送到 PKI 入口。

b）PKI 入口的响应是 HTTP 代码 401"未授权"，该代码中包含一个 WWW-Authenticate 头。该字段指示 UE 使用 HTTP Digest authentication。UE 生成另外一个 HTTP 请求来申请 CA 证书。UE 应在 URL 请求中指出 CA 发放者 的姓名，如 WPKIOMA："无线应用描述；公钥基础设施定义"。

c）第 7.4.1 节所规定的那样。应忽略序列号字段。通过使用标识符和会话密钥 Ks_NAF 来计算 Authorization 头的值。并不一定要对该 HTTP 请求进行认证，认证的目的是遵从 HTTP Digest authentication 的规定。另外，需要把标识符传送到 PKI 入口。

d）CA 证书发送请求的格式应如下所示：

GET <base URL>?in=<issuer name>[other URL parameters] HTTP/1.1

其中，

<base URL>　标示一个服务器或程序。

<issuer name>标识证书发放者，是对 X.509 证书中的 DER 编码的发放者字段进行 base64 编码。

[其他 URL 参数] 是附加的、可选的 URL 参数。

e）PKI 入口接收到请求后，可以使用标识符从 bootstraping 服务器取回会话密钥 Ks_NAF 来验证 Authorization 头。PKI 入口将生成一个包含 CA 证书的 HTTP 响应，并通过会话密钥 Ks_NAF 来对使用 Authentication-info 头的 HTTP 响应进行认证和完整性保护。事实上，该响应可以使用 HTTP 格式的其他发送协议，比如包含内容类型 signedData 的 PKCS#7 加密消息。

f）HTTP 响应包含 CA 证书。CA 证书应进行 base64 编码，以如下格式分界：

HTTP/1.1 200 OK

Content-Type：application/x-x509-ca-cert

-----BEGIN CERTIFICATE-----

<base64 encoded X.509 certificate blob>

-----END CERTIFICATE-----

g）当 UE 接收到新的 CA 证书时，它必须激活 Authentication-info 头。如果成功激活，用户将被告知一个新的 CA 证书投入使用。如果用户接受新的 CA 证书，该证书将被存储入本地的证书管理系统，并被标为“可信任的” CA 证书。

6.1.7 预验证密钥对或者预共享密钥的作用

6.1.7.1 预验证密钥对

除了基于AKA和自举功能来保护证书登录外，还有一种替代办法，就是基于UE中的预验证密钥的签名来保护证书登记。这种方法已经在OMA（见WPKI第7.3.4节）中定义，因此不在本规范之内。下文将简略解释UE中预验证密钥对的作用。

在这种替代办法中，预先发放配备了UICC的UE，带有来自归属网络的预装的、长期的公/私密钥对。这一阶段的操作以带外（out of band）方式进行，其结果是UE具有一对存储在UICC中的长期密钥对，用于认证证书请求。OMA通过WPKI 规范和WIM 规范为存储和使用长期的密钥对提供了标准化的方案。USIM和WIM就是在UICC上应用实例，UICC能够处理长期密钥对。

UE能够通过使用所管理的长期密钥向CA发送证书请求，请求中包括来源证明（例如私钥是存储在WIM中的）。证书请求自身可能包含一个新生成的、需要CA验证的公钥。假定新的密钥对在UICC中产生。对预装的长期私钥的访问控制的安全性至少宜与USIM的访问控制同样好。

管理性的长期私钥的证书总是长期证书，该私钥提供所生成的密钥的来源证明。另一方面，WIM中生成的用户密钥可能有短期或者长期的证书，这取决于CA的策略（见OMA's WIMOMA：“无线身份模块；安全”，WPKIOMA：“无线应用描述；公钥基础设施定义”和ECMA scriptOMA：“ECMAScript移动文件的密码对象”规范）。

6.1.7.2 对称的预享密钥

同上所述，但是提供所生成密钥的来源证明的管理性密钥是一个共享的对称密钥，在这种场景下，它并没有证书（见OMA's WIM OMA：“无线身份模块；安全”，WPKIOMA：“无线应用描述；公钥基础设施定义”和ECMA scriptOMA：“ECMAScript移动文件的密码对象”规范）

注：本章中所讨论的预共享对称密钥和与GBA相关的共享密钥不同。

标准分享网 www.bzfxw.com 免费下载

7 UE 采用 HTTPS 接入 NAF

本章说明了在GAA中实现网络应用功能模块的安全接入的一种方式，这种方式是利用HTTP加TLS的方式来实现。同时，文档还提供了阶段2的安全需求，原则和接入过程。本部分描述了直接接入应用服务器（AS）和通过认证代理（AP）间接接入两种方式。

注：任何有关应用服务器接入应用的具体细节不在本规范范围内，而包括在其他文档中。如描述表现服务安全的3GPP TS 33.141。

7.1 安全构架概述

整体安全构架与第5章中定义一致。有关有认证代理的解决方案的细节将在第7.3节给出。

7.2 认证机制

7.2.1 接口模型

图20描述了使用启动生成秘密信息实体的网络模型，以及实体间的接口点。

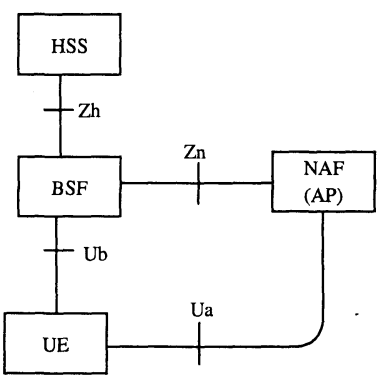


图20 使用自举服务的 NAF 高层参考模型

7.2.2 一般要求和原则

本文档基于第5章定义的架构。所有没有解释的概念都可以在第5章中找到。在本文中KS_(ext)_NAF表示UE和NAF间共享的密钥。在GBA_U中，KS_（ext）_NAF表示KS_ext_NAF；在GBA_ME中，KS_（ext）_NAF表示Ks_NAF。

UE应该可以指示NAF哪一种密钥（Ks_ext_NAF或Ks_int_NAF）它要用来保护Ua口的HTTPS。

签约用户归属网络的运营商应该能够请求某一种密钥（即Ks_ext_NAF或Ks_int_NAF）用来保护UE和NAF之间的HTTPS接入。这样的归属运营商控制使用USS。

7.2.2.1 对 UE 的要求

为了如本文所述来利用GBA，终端UE必须配备具有HTTPS功能的客户端（比如浏览器），并且客户端还必须实现如第5章所述的GBA功能。

UE负责HTTPS客户（即HTTP客户和TLS客户）。HTTP客户和TLS客户存在于ME或UICC。HTTPS客户存在于ME或者UICC，或者ME和UICC分别负责一个HTTPS客户。当HTTPS客户应用于ME时，Ks_ext_NAF应该使用在UE和NAF之间作为共享密钥。当HTTPS客户应用于UICC时，Ks_int_NAF应该使用在UE和NAF之间作为共享密钥。

7.2.2.2 对 NAF 的要求

为了如本文所述来利用GBA，NAF必须支持如第5章所述的GBA功能。

NAF应该有可能被配置基于哪种密钥限制服务接入，（如只允许存在于UICC的那些HTTPS客户接入和使用Ks_int_NAF）。USS里的密钥选择指示要高于NAF本地策略。

注意：对于NAF，对GBAZ-U的支持是可选的。但是，如第5章所示，NAF支持Ks_ext_NAF的使用，而Ks_ext_NAF是GBA_U无关的。

另外，在此规范中，NAF在UE-NAF接口上必须支持HTTP和TLS。

NAF应对是否接受2G签约用户有自己的策略。

7.2.3 基于共享密钥的UE认证和基于证书的NAF认证

对于基于ME的应用，本部分所描述的认证机制强制应用在ME和NAF里。

对于基于UICC的应用，本部分所描述的认证机制选择应用在UICC和NAF里。

这部分解释了当ME和NAF之间，或者UICC和NAF之间采用HTTPS时，如何来加强第5章中描述的过程。下面部分是对第5章中的过程的补充描述。本文定义了某些报头域所携带的逻辑信息。在NAF的GBA_U（即应该使用Ks_ext_NAF还是Ks_int_NAF）情况，报头域确切的定义和密钥选择逻辑是TS29.109和TS24.109的一部分。在下文中，HTTPS客户存在于ME或者UICC。

1）当HTTPS客户通过Ua接口与NAF开始通信时，它必须首先与NAF建立一个TLS隧道。NAF通过公钥证书向UE认证。HTTPS客户必须验证服务器的证书与它所建立隧道的FQDN一致。TLS中的用户认证部分没有被执行。（用户证书是不必要的）

2）HTTPS客户在TLS隧道（HTTPS，即基于TLS的HTTP）内向NAF发送HTTP请求消息。HTTPS客户必须向NAF说明它支持基于GBA的认证，这通过在“User-Agent”HTTP报头中加入常量字符串作为产品标记来支持的，如IETF RFC2616所述。这个常量字符串对基于ME的应用是“3gpp-gba”或者对于基于UICC的应用来说是“3gpp-gba-uicc”。UE要将NAF的主机名在“Host”HTTP头中发送。

注 1：如果NAF可以用不同的主机名进行编址，能够发送NAF主机名的能力尤为重要。否则，NAF将不能辨认HTTPS客户是在与哪个NAF进行连接。BSF在密钥生成中也需要主机名。

如果签约用户是2G用户，那么HTTPS客户应在“User-Agent”HTTP头中加入一个长串“3gpp-gba-2G”作为指示NAF其是2G签约用户的标志，如IETF RFC2616所述。

3）从Ua接口收到HTTPS客户的HTTP请求消息之后，NAF应该调用HTTP摘要，如RFC2617所示，以便执行如第5章所定义的使用共享密钥的客户端验证过程。

NAF首先验证接收到的HTTP请求里的应用类型（基于ME应用的“3gpp-gba”或者基于UICC应用的“3gpp-gba-uicc”）。接着，NAF验证是否伴随WWW-认证头域的正确的域属性被使用，即域属性应该包括常量字符串“3GPP-自举”（基于ME应用的情况）或者“3GPP-bootstrapping-uicc”（基于UICC应用的情况）并且NAF的FQDN（两种情况都有）应该指示GBA作为请求认证的方法。

如果NAF配置禁止请求的GBA模式接入服务（如当这个服务的NAF配置请求Ks_int_NAF应该被使用，但是HTTP请求包含“3gpp-gba”），或者如果NAF不支持请求的GBA模式（即，当NAF是GBA_U情况，收到了在“User-Agent”HTTP头中的HTTP请求是“3gpp-gba-uicc”），那么，NAF应该响应适当的错误代码，并且终止和UE的TLS连接。

如果NAF收到的HTTP请求包含“3gpp-gba-2G”，但是NAF根据本地策略不给2G签约用户提供服务，那么NAF应响应适当的错误代码，并且终止与UE的TLS连接。

标准分享网 www.bzfxw.com 免费下载

4）收到NAF的应答消息之后，HTTPS客户必须验证realm属性中的FQDN与所建立的TLS连接中的NAF的FQDN一致。如果验证失败，HTTPS客户将终止与NAF的TLS连接。

5）在随后的对NAF的请求消息中，HTTPS客户发送的应答中包括一个授权报头域，其中摘要部分使用B-TID作为用户名。NAF衍生密钥（在基于ME的应用情况下的Ks_ext_NAF或者基于UICC应用情况下的Ks_int_NAF）在摘要计算里作为密码。

6）收到这个请求之后，NAF必须验证口令属性的值。这一过程是将口令与使用B-TID作为用户名通过Zn接口向BSF询问得到的密钥（Ks_（ext）_NAF或者Ks_int_NAF）比较来完成。

如果NAF请求了一个USS，并且USS指示NAF使用在HTTPS使用Ks_int_NAF，那么NAF应该只接受Ks_int_NAF作为NAF衍生密钥。因此，如果HTTPS客户使用Ks_（ext）_NAF作为NAF衍生密钥，则NAF要以适当的错误代码作为响应，并且终止与UE的TLS连接。

如果BSF向NAF指示用户为2G签约用户，并且BSF或NAF根据本地策略决定NAF不向2G用户提供服务，那么NAF应响应适当的错误代码，并终止与UE的TLS连接。

7）完成第6）步之后，UE和NAF作为TLS隧道的终点进行了双向认证。

注 2：RFC 2617中第三部分规定发往同一域的HTTP请求必须包含授权请求报头域，否则服务器必须发送一个新的有WWW-Authenticate报头的“401 Unauthorized”消息。原则上说没有必要因为安全的原因在每一个新的HTTP请求后都发送一个授权报头，只要TLS隧道存在。但是，这样会与RFC 2617不一致。

另外，TLS会话的生命周期也会存在问题，因为TLS会话可能在不可预测的时间内过期（至少对UE是这样的），所以UE发送的任何请求都可能是新建立的TLS隧道的第一个请求，而这要求NAF重新检查用户的身份。

AP/AS应能请求一个活动的UE进行重新验证，见第5章。

关于密钥存储内容可参见附录F。

7.2.3.1 TLS 描述

UE和NAF必须支持RFC 2246和WAP-219-TLS中的TLS版本或者更高的版本。

注 1：根证书的管理不属于此规范的范围。

UE和NAF必须支持服务器名称TLS扩展。其他的RFC 3546中的TLS扩展在实现过程中是可选的。

注 2：如果NAF是基于虚拟名称的主机服务，那么NAF要么需要一个包含所有支持的主机名的TLS服务器证书，要么需要为每一个主机名申请一个证书。在后面一种情况下，服务器名字扩展项是需要的，因为NAF需要能够选择正确的TLS服务器证书。

7.2.3.1.1 保护机制

UE必须支持密码包TLS_RSA_WITH_3DES_EDE_CBC_SHA和TLS_RSA_WITH_AES_128_CBC_SHA其他的RFC 2246和RFC 3268中定义的密码包在UE的实现中是可选的。

NAF必须支持密码包TLS_RSA_ WITH_3DES_EDE_CBC_SHA以及加密包TLS_RSA_WITH_RC4_128_SHA和TLS_RSA_WITH_AES_128_CBC_SHA。其他的RFC 2246和RFC 3268中定义的密码包在NAF的实现中是可选的。

也可能选用加密项为空的密码包。UE必须至少包括一个支持握手过程中加密的密码包。

不允许完整性保护（或者HASH）为空的密码包。

7.2.3.1.2 密钥协商

密钥交换算法必须是非匿名的。因此，会话保护中不允许使用如下的RFC 2246中的密码包：

CipherSuite TLS_DH_anon_EXPORT_WITH_RC4_40_MD5

CipherSuite TLS_DH_anon_WITH_RC4_128_MD5

CipherSuite TLS_DH_anon_EXPORT_WITH_DES40_CBC_SHA

CipherSuite TLS_DH_anon_WITH_DES_CBC_SHA

CipherSuite TLS_DH_anon_WITH_3DES_EDE_CBC_SHA

7.2.3.1.3 AP/AS 的认证

AP/AS如WAP-219-TLS所示过程向客户端认证，这个文档基于RFC 2246。

AP/AS证书格式必须基于WAP 211 WAPCert的WAP证书和CRL格式。

7.2.3.1.4 认证失败

如果UE收到一个来自要求证书的AP/AS的Server Hello 消息，UE必须应答一个不包含证书的证书消息如果UE没有证书。AP/AS收到这个消息之后可能发送一个失败警告，但是如果AP/AS根据运营商的测量必须对用户认证，那么AP/AS必须继续会话并且假设UE将会被第5章中所示的过程认证。

如果从网络发起重认证请求之后指定时间内网络中没有应答消息，并且请求消息在发送了指定次数之后仍没有消息，那么认证失败。可以有多个原因造成认证失败。比如，UE关机或者信道太差以致消息丢失。AP/AS必须仍然假设TLS会话仍然是有效的并且可以在以后的会话中被UE重新使用。只要UE重新使用现存的会话，AP/AS必须重新认证用户并且不允许用户接入AP/AS，除非认证成功。

7.2.3.1.5 安全参数的建立

TLS握手协议发起一个会话，会话用会话ID来标识。客户端和AP/AS必须允许重新利用会话。这样使得客户和服务器可能继续一个先前的会话或者复制一个现存的会话。会话ID的生命周期最长是24小时。会话ID只可以在生命周期内被使用，当生命周期结束后，它在客户端和服务器端都被认为是无效的。

7.2.3.1.6 错误情况

AP/AS必须认为如下情况为严重错误：

如果收到的密码包只包括所有或者部分在7.2.3.1.2中所提到的包。

如果收到的密码包不包括任何完整性保护。

7.2.4 基于共享密钥的 UE 和 NAF 的双向认证

对于基于ME的应用，本部分所描述的认证机制选择应用在ME和NAF里。

对于基于UICC的应用，本部分所描述的认证机制选择应用在UICC和NAF里。

HTTP客户端和服务器端可以基于在启动过程中生成的共享密钥进行互相认证。共享密钥必须作为主密钥生成TLS会话密钥，并且作为认证函数中拥有密钥的证明信息。确切的过程在Pre-Shared Key Ciphersuites for Transport Layer Security （TLS）中有描述。

这部分解释了从如第5章所示的UE和NAF建立的共享密钥是如何与IETF Inernet-Draft的Pre-Shared Key （PSK）密钥包结合使用的。HTTPS客户可以存在于ME和UICC中。在前一种情况，Ks_（ext）_NAF应该用来建立TLS会话密钥。后一种情况，Ks_int_NAF应该用来建立TLS会话密钥。

a）当 UE 与 NAF 联系时，它可能通过在 ClientHello 消息中添加一个或者多个基于 PSK 的密钥包来告诉 NAF 它支持基于 PSK 的 TLS。UE 在 ClentHello 消息中必须包括其他非基于 PSK 的密钥包。UE 必须在 ClientHello 消息中用服务器名称扩展项来发送 NAF 主机名，如 RFC 3546 所示。

标准分享网 www.bzfxw.com 免费下载

注 1：能够发送NAF主机名的能力尤为重要如果NAF可以用不同的主机名进行编址。否则，NAF将不能辨认UE是在与哪个NAF进行连接。BSF在密钥生成中也需要主机名。

注 2：当UE在ClientHello消息中加入一个或多个基于PSK的密钥包时，这被认为是表示UE支持基于PSK的TLS。如果UE支持基于PSK的密钥包但不支持基于GBA的认证，那么TLS握手过程就会失败如果NAF选择了基于PSK的密钥包并且建议使用GBA（如第二步所示）。在这种情况下，UE必须尝试在ClientHello消息中不包括基于PSK的密钥包来建立TLS连接，过程如7.2.3中所示。这点并将PSK TLS的使用局限与基于HTTP的服务。

如果 NAF 愿意使用基于 PSK 的密钥包来建立 TLS 隧道，那么它选择 UE 提供的一个基于 PSK 的密钥包，并在 ServerHello 消息中将选择的密钥包发送给 UE。NAF 会随着 PSK-身份标志发送 ServerKeyExchange 消息。常量字符串“3GPP-bootstrapping”作为PSK-身份标志来指示NAF里的本地配置，即 NAF 接受 Ks_（ext）_NAF 用来建立 TLS 会话密钥。常量字符串“3gpp-bootstrapping-uicc”用来作为 PSK-身份标志来指示 NAF 的本地策略接受 Ks_int_NAF 作为 TLS 会话密钥。这些 PSK-身份标志之一应该在 ServerKeyExchange 消息里面，它应该作为请求认证方法指示 GBA。如果 NAF 的本地配置允许使用 2 种认证方法接入服务，那么 ServerKeyExchange 消息应该包含 2 种 PSK-身份标志，即一个身份标志包括“3gpp-bootstrapping”，另一个包括“3gpp-bootstrapping-uicc”。其他的 PSK-身份标志可以被支持，然而，超出了本部分范围。NAF 结束响应给 UE 发送 ServerHelloDone 消息。

注：如果 NAF 不希望使用基于 PSK 的密码包来建立 TLS 隧道，它必须选择一个非基于 PSK 的密码包并继续 TLS 的建立过程，基于 7.2.3 或 7.2.5 的过程。

b）如果 NAF 已经发送了包含一个基于 PSK 的 ServerHello 消息和包含字符串“3gpp-bootstrapping”或者“3GPP-bootstrapping-uicc”，或者两者的 ServerKeyExchange 消息作为 PSK 标识信息，UE 必须使用基于 GBA 的共享秘密信息来建立 PSK TLS。如果 UE 没有有效的基于 GBA 的共享秘密信息，它必须通过 Ub 接口与 BSF 运行启动过程来获得一个，如第 5 章所示。

如果 HTTPS 客户存在于 ME 中，Ks_（ext）_NAF 应该作为 GBA 共享密钥使用。如果 HTTPS 客户存在于 UICC 中，则 Ks_int_NAF 应该作为共享密钥使用。

如果签约用户时 2G 用户，并且用户收到指示 NAF 不接受 2G 用户，那么 HTTPS 客户应中止与 NAF 的通信。

UE 从 NAF 衍生密钥（如果初始 HTTPS 客户存在于 ME 则是 Ks_（ext）_NAF，或者如果初始 HTTPS 客户存在于 UICC 则是 Ks_int_NAF）衍生出 TLS 预主密钥，如 RFC4279 描述。

UE 必须发送一个 ClientKeyExchange 消息。该消息中的 PSK 标识必须包括一个前缀来说明选择的 PSK 标识（即“3GPP-bootstrapping-uicc”或者“3gpp-bootstrapping”）空间和 B-TID。这个前缀必须与 NAF 在 ServerKeyExchange 消息中提供的某个 PSK 标识信息相同。PSK 的准确格式在 TS 24.109 中描述。

c）如果 NAF 收到 ClientKeyExchange 消息中的“3gpp-bootstrapping”前缀和 B-TID，它使用 B-TID 从 BSF 中获取特定的共享密钥（Ks_（ext）_NAF），否则 NAF 收到 ClientKeyExchange 消息中的“3gpp-bootstrapping-uicc”前缀和 B-TID，它使用 B-TID 从 BSF 中获取特定的共享密钥（Ks_int_NAF）。

如果 BSF 指示 NAF，用户是 2G 签约用户，但是 BSF 或 NAF 根据本地策略决定 NAF 不接受 2G 签约用户，NAF 应响应适当的错误编码，并且终止 Ua 口的协议。

如果NAF要求USS，并且USS指示NAF只有Ks_int_NAF允许，那么NAF只能接受Ks_int_NAF作为NAF衍生密钥。如果这时Ks_（ext）_NAF用来作为NAF衍生密钥，则NAF响应适当的错误编码，并且终止与UE的TLS连接。

NAF从NAF的特定密钥（Ks_（ext）_NAF或者Ks_int_NAF）来获得TLS的预主秘密信息，如IETF Inernet Draft所示。

NAF发送ChangeCipherSuite和Finished消息给UE来结束TLS握手过程。

UE和NAF已经通过使用基于GBA的共享秘密信息建立TLS隧道，然后他们就可以利用这个隧道来允许应用层的对话。

7.2.4.1 TLS描述

如果支持基于PSK TLS的认证机制，在UE和NAF的HTTPS客户必须支持如RFC 2246，WAP 219 TLS，PSK中定义的TLS版本，或更高的版本。更早的版本不被允许。

在UE和NAF的HTTPS客户必须支持服务器名TLS扩展项。RFC 3546中的其他的扩展项在实现中是可选的。

注：如果NAF支持虚拟主机名机制（比如在有认证代理情况下，请看附录A），NAF需要能够分辨出正确的服务器名称来告诉BSF正确的NAF_ID。否则，BSF将不能得到正确的NAF衍生函数。

7.2.4.1.1 保护机制

UE必须支持密钥包TLS_PSK_WITH_3DES_EDE_CBC_SHA 和 TLS_PSK_WITH_AES_128_CBC_SHA。PSK TLS中其他的密钥包在实现中是UE可选的。

NAF必须支持TLS_PSK_WITH_3DES_EDE_CBC_SHA，TLS_PSK_WITH_RC4_128_SHA和TLS_PSK_WITH_AES_128_CBC_SHA。PSK TLS中其他的密钥包在实现中是NAF可选的。

加密部分为空的密钥包是可以选用的。UE必须提供至少一种支持握手过程中加密的密钥包。

完整性保护（或者Hash）为空的密钥包是不允许的。

7.2.4.1.2 AP/AS认证

AP/AS如PSK TLS所示的过程向客户端认证。

7.2.4.1.3 认证失败

如果从网络发起重认证请求之后指定时间内网络中没有应答消息，并且请求消息在发送了指定次数之后仍没有消息，那么认证失败。可以有多个原因造成认证失败。比如，UE关机或者信道太差以致消息丢失。AP/AS必须仍然假设TLS会话仍然是有效的并且可以在以后的会话中被UE重新使用。只要UE重新使用现存的会话，AP/AS必须重新认证用户并且不允许用户接入AP/AS，除非认证成功。

如果AP/AS作为NAF请求了USS，并且USS指示NAF只有Ks_int_NAF允许，那么NAF只能接受Ks_int_NAF作为NAF衍生密钥。如果这时Ks_（ext）_NAF用来作为NAF衍生密钥，则NAF响应适当的错误编码，并且终止与UE的TLS连接。

7.2.4.1.4 安全参数的建立

TLS握手协议发起一个会话，会话用会话ID来标识。客户端和AP/AS必须允许重新利用会话。这样使得客户和服务器可能继续一个先前的会话或者复制一个现存的会话。会话ID的生命周期最长是24小时。会话ID只可以在生命周期内被使用，当生命周期结束后，它在客户端和服务器端都被认为是无效的。

7.2.5 基于证书的UE和应用服务器的双向认证

标准分享网 www.bzfxw.com 免费下载

本部分所述的认证机制在UE和AS实现是可选的。

基于证书的UE和应用服务器的双向认证必须基于IETF RFC 2246和IETF RFC 3546的TLS。

附录M中提供了这个过程的指南。

7.3 认证代理的使用

认证代理AP是一个HTTP代理，它对UE提供NAF的作用。它处理与UE的TLS安全关系，将应用服务器AS从这个工作中解放出来。基于GBA技术，AP可以向AS确认请求是来自MNP授权的的用户。

7.3.1 架构

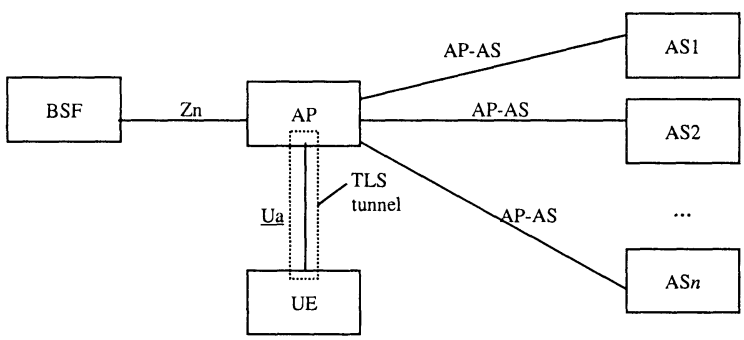


图21 AP 的环境和接口

认证代理的使用完全与 TS33.220 的构架兼容。当 AP 应用与这个构架中时，AP 取代了 NAF 的角色。当一个 HTTPS 请求是发向 AP 所代理的 AS 时，AP 完成 TLS 隧道并且执行 UE 认证。AP 为一个或者多个 AS 做 HTTP 请求代理。当 AP 将请求消息转发给 AS 时，AP 可能添加一个用户身份的确认信息给 AS。

注：一个例子，下面的情况允许通过一个共享的TLS隧道（通过Ua接口）ASnhostname=AP hostname=NAF_ID来接入多个AS。也许存在其他的接入AP代理的多个AS的的方式。

图22描述了一个使用AP的构架，比如，对于基于IMS SIP的服务。UE必须通过Ua/Ut接口来管理自己的数据如组信息等。TS 23.002中定义的Ut接口必须可用于基于SIP的IMS服务数据操作管理，比如Presence，消息和会议服务。阶段1的需求在TS 22.250中有描述。

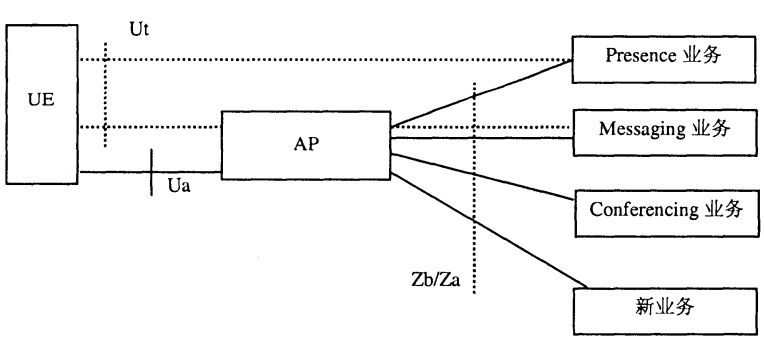


图22 AP 应用于基于 IMS SIP 服务的构架

UE身份的管理在7.3.5节中描述。

附录G 包括AP技术解决方案的指南。

7.3.2 要求和原则

认证代理可以位于UE和AS的中间位置如图21所示。认证代理的用处可以简化到认证向量的消耗和减小SQN同步失败。另外，AP解除了AS的安全工作。

认证代理的使用有如下的要求：

1）认证代理必须能够使用GBA来对UE进行认证，如第5章所述；

2）如果应用服务器要求UE的认证身份信息，认证代理必须在每个HTTP请求中将其发送给信任域的应用服务器；

3）如果要求，认证代理可以不向非信任域的应用服务器提供UE的认证身份；

4）认证身份管理机制不能妨碍应用服务器与用户使用适当的会话管理机制；

5）UE必须能够通过认证代理生成与多个不同的应用服务器并行的HTTP会话；

注 1：会话管理机制不属于3GPP规范的范围。

注 2：在UE和AS间采用AP的一个原因是减少TLS连接的个数。但是，会存在UE和AP停止并行TLS连接的情况，比如，UE的2个应用不能够共享TLS连接。

6）AS中检查用户身份的机制是可选的；

7）是否要求传送用户身份的要求是可以在AP中为每一个AS 进行设置；

8）认证代理的使用必须使得在UE端不必进行设置管理。

注 3：这个要求意味着认证代理必须是具有下面意义的反向代理：一个反向代理是一个网络服务系统，这个系统除了可以提供硬盘上或者动态的有CGI生成的网页，还可以提供来源于其他服务器的网页，并且使得这些网页看起来就像来源于反向服务器本身。

7.3.3 接口

7.3.3.1 Ua 接口

Ua 接口在规范第 5 章中有标准定义。

注：可选的AP的引入具有的优点将在其他地方描述。但是，下列影响必须被考虑以决定是否引入AP：

AP结束了TLS和HTTP摘要。这使AS摆脱了处理TLS和HTTP摘要的工作，但是必须注意到UE不能与AS建立另外的端对端的TLS隧道，并且也不能通过TLS的客户端认证来向AS直接认证。更进一步，如果GBA认证使用HTTP摘要认证，那么UE与AS不能使用基本的或者直接的摘要认证。

7.3.3.2 AP-AS 接口

AP-AS接口使用的HTTP协议。

AP和AS间的机密性和完整性保护可以通过NDS/IP机制来完成，如TS 33.210所示。不同安全域间的通信使用Za接口。同一个安全域间的通信，取决于运营商是否采用Zb接口。既然AP终结了TLS通道，采用TLS通道也是可行的。

AP可能支持认证了的UE的身份信息在AP之间以一种标准的方式进行传播。在HTTP请求报头中这些信息的格式将留到第三阶段的规范中处理。

7.3.4 UE 身份的管理

不同的AS需要不同的认证信息。为了支持不同服务器的要求，AP需要执行不同粒度和不同声明程度的认证。认证和相应的声明是针对AS的，因此应该是在AP中对每个AS进行单独设置。

7.3.4.1 AP 的认证粒度和接入控制

AP是对每个AS单独设置的，如果对于特别的应用或者AS提供的应用需要单独的用户安全设置，请看第5章。这个用户安全设置可以包括用户在USS认证部分的公开身份。USS的认证部分可能包括诸如用户可以接入的AP提供的应用，AP代理的AS等。

7.3.4.1.1 授权的 GBA 参与者

标准分享网 www.bzfxw.com 免费下载

AP检查UE是否授权的GBA参与者。用户被授予接入权限如果GBA过程成功执行，即，在UE的HTTPS客户发送有效的B-TID并且使用从BSF得到的NAF衍生密钥执行摘要认证。

AP被设置成不要求应用为请求信息中的AS从BSF中请求应用独立的用户安全设置。倚赖于BSF的具体设置，AP可能收到用户的私有身份（IMPI）。

AP必须支持这种情况。

注：这种情况可能应用于某个运营商所有的的注册用户，但是不包括其他任何用户，被允许接入运营商定义的服务。从私密性考虑或者AP不需要的情况下，BSF也许不发送IMPI。如果BSF不发送IMPI给AP，那么用户对于AP是匿名的，后者更确切地说，B-TID作为用户的临时名称。

7.3.4.1.2 应用的授权用户

AP被设置成需要从BSF获取应用独立的用户安全设置。倚赖于BSF的策略，AP从BSF收到了应用独立的用户安全设置和用户私有身份。接入的许可倚赖于从BSF得到的应用独立的用户安全设置。

如果要求的话，AP可能对用户HTTP摘要中的信息做进一步的检查，如7.3.5.2.4。

AP必须支持这种情况。

注：如果某个应用不存在应用独立的用户安全设置，那么这种情况简化成7.3.5.1.1的情况。

7.3.4.2 确认身份从 AP 到 AS 的传递

为每个AS设置AP ，使得AP根据如下的要求来运行认证和接入控制：如果有要求，在每一个转发的HTTP请求中都传送了用户身份。

7.3.4.2.1 GBA 的授权参与者

AP检查UE是否合法的GBA参与者。如果AP对UE的认证失败，那么AP不再向AS转发UE的请求。

AP必须支持这种情况。

注意：这种情况意味着NAF检查用户是BSF已知的并且与通过GBA过程与BSF建立了有效的密钥，如第5章所示。

7.3.4.2.2 AS 匿名应用的授权用户

AP检查根据从BSF获取的应用独立用户安全设置来检查UE是否授权用户。不能传输任何用户身份给AS。

AP必须支持此种情况。

7.3.4.2.3 传送用户身份确定的授权用户

AP检查UE是否应用的授权用户。从BSF获取的用户身份必须传送给AS。基于AS独立的AP的设置，应用独立的用户安全设置中任何的授权标志也必须传送给AS.

依赖于应用独立的用户安全设置和AS独立的AP 设置，传送的用户身份可以是IMPI，或者是某个应用中用户的身份（比如IMPU），或者是AP选择的假名（比如Random，B-TID）。

AP必须支持这种情况。

注 1：如果AP被设置成传送假名给AS，假名与用户身份的绑定不是本规范的范围。

注 2：如果AP被设置成不需要从BSF获取应用独立的用户安全设置，只有IMPI或者假名被传递给AS。这种情况下，任何GBA的授权用户被默认为应用的授权用户。

7.3.4.2.4 传送身份确认的应用授权用户和用户插入身份检查

这种情况与7.3.5.2.3类似，并有如下扩展：

基于从BSF获得的用户身份，AP通过UE发送的身份信息元素来鉴别用户。用户插入身份可以出现在报头域或者是HTTP请求内。

依赖于应用独立的用户安全设置和AS独立的AP设置，所有的用户插入身份通过IMPI或者应用独立的用户安全设置来进行检查。

依赖于应用独立的用户安全设置和AS独立的AP设置，传送的用户身份可以从用户插入身份中选择。

AP必须支持这种情况。

注 1：如果AP认证某些或者所有的请求中用户有关的身份信息，AS必须依赖于这些元素的检查，那么AP和AS之间相应的策略需要制定。

注 2：任何应用具体细节超出了本规范的范围，可以在应用中具体制定，比如，3GPP TS 33.141.本规范不排除其他应用规范中将这些特征设置为必选项。

8 通用认证框架 Push 功能

8.1 概述

GBA-push是一种机制，可以不需要驱使UE去联系BSF发起自举而在NAF和UE之间建立安全关联。

8.2 GBA Push 架构描述及基本原理

GBA push功能建立在3GPP TS33.220（对应于第5章）的架构和功能上。与3GPP TS33.220主要的区别是在BSF和NAF，NAF和UE之间定义了新的参考点。基本原理如下图所示。

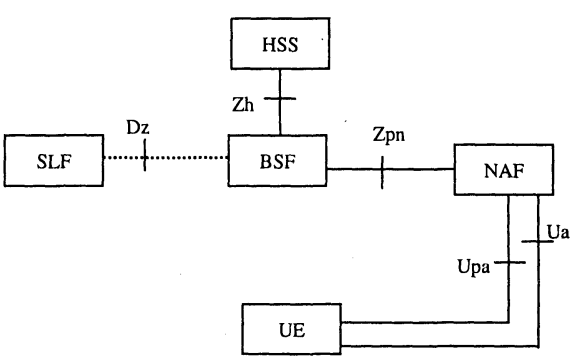


图23 通过 NAF 推送自举的简单网络模型

图23所示GBA架构基于以下基本原理：

1）应不影响 Ua 参考点保护，即不管 GBA 密钥是 UE 发起的还是 push 发起的，都不应对 Ua 协议产生任何不同。因此，引入了另一个参考点 Upa，这个参考点负责推送 GBA 消息（称为 GBA-PUSH-INFO）给 UE。

2）就 BSF 来看，NAF 始终是密钥取回的发起实体，除了在 NAF 没有 B-TID 的情况下（但是 UE 可以有有效的 GBA 会话）。引入了一个 Zpn 参考点，重用 Zn 参考点协议定义在 TS33.220（第 5 章）。

3）Ub 参考点是 UE 发起的，并且应用 HTTP digest AKA。GBA 推送信息，即 GBA-PUSH-INFO，希望不要使用 HTTP 传送，因为这样需要 UE 运行 HTTP 服务器。在 NAF 和 UE 之间的新的参考点 Upa 是网络发起的，由它来定义 GBA-PUSH-INFO。NAF 通过 Zpn 接口从 BSF 收到 GBA-PUSH-INFO。

4）应该有可能使用 Rel 6 的 UICC，即引入了 GBA push 网络功能，智能卡上的 GBA 功能（如 GBA_U）不需要做任何改变。

标准分享网 www.bzfxw.com 免费下载

8.3 GBA Push 需求

8.3.1 通用 GBA Push 需求

以下为GBa push可实用要求：

1）网络实体应该能够安全地触发自己与 UE 之间的安全关联建立。

2）网络实体应该可以给 UE 发送安全的消息（包括延期的消息），其消息能够使 UE 建立共享安全关联。

3）UE 最好不要联系任何网络实体来建立安全关联并检查消息。

8.3.2 参考点 Upa 上的要求

参考点Upa的要求：

1）UE 应该能够识别 push 的发起者，即 BSF;

2）UE 应该能够基于 AKA 鉴别网络（即 BSF）；

注 1：NAF由Ks_（ext/int）_NAF间接地认证（即BSF认证NAF）。

3）BSF 应该能够发送 B-TID 给 UE;

4）UE 和 BSF 应该建立共享密钥;

5）BSF 应该能够指示 UE 密钥的生命周期。BSF 通过 Upa 发送的密钥生命周期应该指示密钥的过期时间。密钥生命周期的传送应该进行完整性保护。

注 2：Upa参考点的要求基于Ub参考点的要求。

6）网络实体应能够指示移动用户在GBA_U的情况下使用哪种密钥（Ks_ext_NAF或Ks_int_NAF）。

编者注：宜检查一下在TS29.109里定义的密钥指示是否已包含了这个要求。如果包含了，则不需要此要求，需要替换成一个参考。

8.3.3 参考点 Zh 上的要求

Zh参考点的要求见TS33.220（4.3.3）。

8.3.4 参考点 Zpn 和 Zpn'的要求

参考点Zn的要求：

1）相互认证，可以提供保密性和完整性;

2）如果BSF和NAF在同一个运营商的网络内，基于参考点Zpn的DIAMETER协议应该根据NDS/IP受到保护;

3）如果 BSF 和 NAF 不在同一个运营商的网络内，在 Zn-Proxy 和 BSF 之间的基于参考点 Zpn'的 DIAMETER 应该利用 RFC 2246 中的 TLS 来保证安全;

注1：附录D详细说明了TLS描述文件。

4）基于 Zpn/Zpn'接口的 HTTP 协议应该使用 RFC 2246 中的 TLS 来保护。

注2：附录D详细说明了TLS描述文件。

5）BSF 应该保证发出请求的 NAF 能够被批准去获得密钥资料和请求的 USS;

6）NAF 应该能够发送密钥资料请求到 BSF，根据 Upa 参考点的使用包含 NAF 公共主机名。BSF 应该能够保证 NAF 有权使用这个主机名，即 Upa 参考点上 UE 得到的 FQDN;

注3：这个要求是将TS33.220（第5章）要求更改了的适用于GBA push的要求。

7）BSF 应该能够发送密钥资料到 NAF;

8）NAF 应该能够从 BSF 中有选择性的获得应用相关的 USS，NAF 能够获得什么 USS 决定于 BSF 的策略和 NAF 通过参考点 Zpn 的请求消息中的指示；

9）NAF 应该能够向 BSF 指示出它所需要的 USS 用于一个或者多个应用；

注 4：如果一些应用只需要应用相关的USS的一个子集，比如说只需要一个IMPU，那么NAF就可以从来自BSF的完整USS中选择这个子集。

10）BSF 应该能够对每一个 NAF 或每一个应用被配置，基于

— 是否签约用户的私人身份，即 IMPI，可能发送给 NAF；

— 是否一个特定的 USS 可能发送给 NAF；

11）如果一个 NAF 向 BSF 请求 USS，但是用户的 GUSS 里面不存在 USS，倘若 BSF 本地策略的条件满足了，这就不会引起一个错误。BSF 应该仅将要求并找到的 USS 发送给 NAF；

12）按照下面的描述来配置一个本地策略是可能的：对于一个相关请求的 NAF，BSF 可能需要一个或者多个应用相关的 USS 在这个用户相关的 GUSS 中，如果条件没有满足，就要拒绝来自 NAF 的请求。为了满足这个本地策略，NAF 不需要通过 Zn 参考点来请求 USS，这些 USS 是 BSF 要求在 GUSS 里面存在的，只需要 BSF 在本地查询 USS 就已经足够了。在发出请求的 NAF 没有要求 USS 的情况下，配置 BSF 也是可能的；

注 5：对于更多的有关本地策略应用的信息见3GPP TS33.220附录J。

13）BSF 应该能够向 NAF 指示出自举的时间和密钥资料的生存期。BSF 通过 Zpn 传递的密钥生存期，应该与 BSF 通过 Upb 传递给 UE 的密钥资料的生存期一样。

编者注：需要进一步研究 Upa 口发送的数据。

注 6：这并不能排除NAF在生存期满之前根据本地策略来更新密钥。

注 7：HSS里面的GUSS中的一个或者多个USS（已经发送到NAF了）被更新，只有当NAF下次从BSF请求USS时，更新过的USS才对NAF起作用（假设BSF已经通过Zh参考点更新了用户的GUSS）。

14）NAF 应该能够指示 BSF 在 Ua 口安全协议的协议标识，BSF 要传送 NAF-ID 给 BSF。

15）NAF 应该能够指示 BSF，一个新的自举被请求。

16）NAF 应该指示用户身份给 BSF。

注 8：Zpn的要求基于TS33.220（第5章）描述的Zn参考点的要求。

8.3.5 参考点 Ua 上的要求

参考点Ua的要求参见TS33.220（4.3）。

8.3.6 Zn-Proxy 的要求

当push NAF在拜访网络而不是归属网络时，拜访NAF应使用在NAF网络里的Zn-Proxy和签约用户的BSF通信（即归属BSF）。Zn-Proxy的要求参见TS33.220（4.3）。

8.3.7 自举事务标识的要求

Bootsrapping事务标识（B-TID）通过参考点Ua ，Upa和Zpn将用户身份和密钥资料绑定。

B-TID的要求：

1）B-TID 应该是全局唯一的；

2）B-TID 应该作为一个密钥标识符来使用，应用在 Ua 参考点上；

3）UE 应该能够从 B-TID 识别出 BSF 来。

标准分享网 www.bzfxw.com 免费下载

注 1：NAF在密钥无效之后，要删除那些符合删除条件的安全关联。

注 2：UE和NAF之间使用GBA还是非GBA认证，不能产生冲突，比如说在同一个命名空间。这种潜在的冲突不能通过通用的方式来解决，因为它依赖于相关的协议和UE与NAF之间所使用的认证机制。这超出了本规范的范围。

对于在UE和NAF之间使用的HTTP摘要认证的例子，下面的这种使用方式也是可能的：〈用户名，密码〉对在一个域内必须是唯一的。由于NAF控制域名，所以它必须确保只有基于域的GBA才能以保留的3GPP域名来进行命名。在特殊的情况下，NAF 要在GBA域内允许基于非 GBA的认证，它必须确保没有基于GBA认证之外的用户使用B-TID格式的用户名。

注 3：B-TID的要求基于TS33.220（5）。

8.3.8 参考点 Dz 的要求

BSF和SLF接口用来得到HSS的地址，其要求与TS33.220（第5章）相同。此接口在单一HSS环境里不需要。

8.3.9 其他要求

不管自举是通过Ub口还是Upa口进行，UE和NAF应该能够在Ua接口使用NAF衍生密钥Ks_（ext/int）_NAF。

注：在UE和BSF之间使用GBA-push机制建立GBA安全关联应该不能限制NAF只为网络发起协议使用衍生安全关联。类似的，UE发起的GBA应该不能限制NAF只为UE发起协议使用衍生安全关联。

8.4 GBA Push 功能

图24描述了当NAF没有有效的NAF衍生密钥，NAF发送数据给UE的情况。另外，UE可能不能直接给BSF进行自举过程或者UE应不能直接与BSF进行自举。UE与BSF之间的自举通过NAF进行。

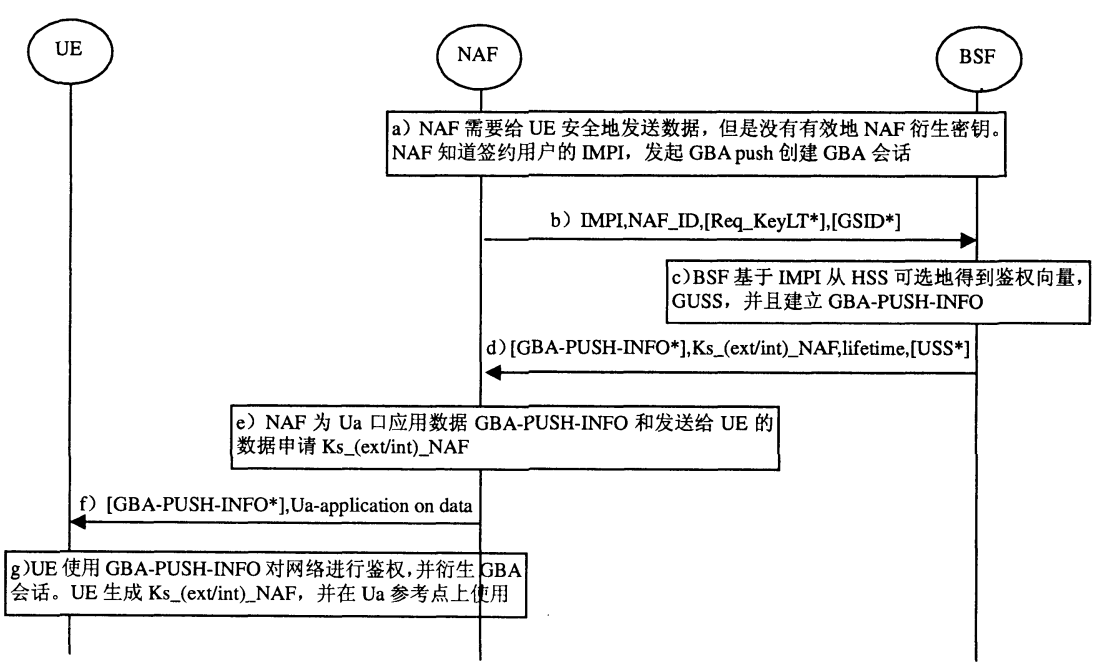


图24 通过 NAF 的自举过程

注 1：UE与网络没有任何连接的情况发生在广播情景。

已经有有效的自举会话，或者需要建立一个自举的过程如下：

a）NAF需要安全地通过Ua口向UE发送数据，但是没有有效的NAF衍生密钥。NAF知道签约用户身份和需要发送给UE的数据。

b）NAF通过Zn口发送签约用户的IMPI，NAF-ID（即NAF主机名和Ua口安全协议标识），并且选择性地发送密钥生命周期（Req_KeyLT）和一个或多个GSID。

c）从NAF收到请求后，BSF检查NAF是否有权进行GBA push，并且签约用户是否有有效的自举会话。

— 如果签约用户有有效的自举会话，那么BSF基于NAF_ID计算出Ks_（ext/int）_NAF和其他的密钥衍生参数如TS33.220（第5章）所述。而且，BSF从签约用户的GUSS提取出请求的USS（如果有的话）。BSF也产生GBA-PUSH-INFO并且将其发送给NAF。

— 如果签约用户没有有效的自举会话，并且NAF有权发起GBA push请求。那么BSF从HSS得到认证向量，基于NAF-ID计算Ks_（ext/int）_NAF和其他密钥衍生参数。而且BSF从签约用户的GUSS提取出请求的USS（如果有的话）。BSF为签约用户建立自举会话，之后可以为其他NAF所使用。BSF也产生GBA-PUSH-INFO并且将其发送给NAF。

d）BSF将B-TID，Ks_（ext/int）_NAF，密钥生命周期，可选的请求的USS（如果有的话）发送给NAF。

NAF可选地接收GBA-PUSH-INFO。BSF可以应用USS进行策略管理和密钥选择，如TS33.220所述（第5章）。

e）NAF使用Ks_（ext/int）_NAF在Ua口安全传送数据。策略管理如TS33.220所述。NAF应在push信息里加入密钥类型用来指示使用哪种密钥解密数据。

f）如果NAF接收到GBA-PUSH-INFO，那么NAF在为Ua口应用申请NAF衍生密钥之前发送此信息。否则直接为NAF想要发送到UE的数据申请NAF衍生密钥。NAF使用其与UE之间的广播通道发送B-TID，NAF_ID，并且可选地发送加密数据给UE。NAF_ID和被加密的数据可以用其他方法保护，但超出本部分的内容。

如果没有有效的自举会话，那么NAF使用其与UE的广播通道发送AUTN，RAND，B-TID，NAF_ID，并且可选地发送被加密地数据给UE。AUTN，RAND，NAF_ID和被加密的数据可以用其他方法保护，但都超出本部分内容。

g）当UE收到GBA-PUSH-INFO后，UE先检查B-TID是否已知。如果是这样的情况，那么此GBA-PUSH-INFO是重复的，可被丢弃。如果GBA-PUSH-INFO中的B-TID未知，则UE衍生出Ks_（ext/int）_NAF。

当UE收到Ua应用信息后，B-TID作为找到或建立NAF衍生密钥的依据。UE应使用NAF指示的密钥解密push数据。

UE保存以后可与其他NAF使用的自举会话数据。

UE在会话有效以及自举会话被创建时，可以一直与其他NAF使用最近创建的自举会话。

标准分享网 www.bzfxw.com 免费下载

附 录 A
（规范性附录）
密钥衍生函数 KDF 的规范

本附录详细说明了密钥衍生函数KDF，这个函数用于GBA和GBA_U的NAF相关密钥衍生。附录中定义的衍生函数作以下的假设：

a）密钥衍生函数的输入参数是任意长度的字符串而不是比特串。

b）一个单一的输入参数的长度不能超过65535字节。

A.1 通用密钥衍生函数

输入参数和他们的长度应该被编码成一个字符串S，如下：

a）每个输入参数的字节数应该编码成一个2字节的字节串。

（1）输入参数Pi的字节数要以范围[0，65535]中的数字*k*表示出来。

（2）Li是将*k*的以2字节表示方式，Li中第一个字节的最高有效位等于*k*的最高有效位，Li最低有效位等于*k*中最低有效位。

例子：如果Pi包含258个字节，则Li将会是2字节字符串0x01 0x02。

b）字符串S应该以*n*个输入参数组成，如下：

S = FC ‖ P0 ‖ L0 ‖ P1 ‖ L1 ‖ P2 ‖ L2 ‖ P3 ‖ L3 ‖... ‖ P*n* ‖ L*n*

其中：

FC是一个字节，用来区分算法的不同实例，

P0是一个静态的ASCII编码字符串，

L0是P0长度的2字节表示方式，

P1……P*n*是*n*个输入参数，

L1……L*n*是相关输入参数的2字节表示方式。

c）最终的输出，比如说衍生密钥等于对字符串S，使用密钥Key进行HMAC-SHA-256的计算结果。

衍生密钥= HMAC-SHA-256（Key，S）

A.1.1 输入参数编码

一个字符串应该根据UTF-8编码规则，编码成为一个字节串，UTF-8编码规则在IETF RFC 3629（2003）详细说明。

A.2 GBA和GBA_U中的NAF相关密钥衍生

在GBA和GBA_U中，密钥衍生函数的输入参数的说明如下：

— FC = 0x01，

— P1 = RAND，

— L1 = RAND的长度是16字节（比如：0x00 0x10），

— P2 = IMPI利用UTF-8编码方式，编码成为一个字节串（参看A.2.1），

— L2 = IMPI的长度是可变的（不能超过65535），

— P3 = FQDN也作为NAF-ID的一部分进行编码，NAF_ID利用UTF-8编码方式，编码成为一个字节串（参看A.2.1），

— L3 = NAF_ID的长度是可变的（不能超过65535）。

第5.1节的Ks_NAF和第5.2节的Ks_ext_NAF的密钥衍生：

— P0 = “gba-me”（例如：0x67 0x62 0x61 0x2d 0x6d 0x65），

— L0 = P0的长度是6字节（列如：0x00 0x06）。

第5.2节的Ks_int_NAF的密钥衍生：

— “gba-u”（例如：0x67 0x62 0x61 0x2d 0x75），

— P0的长度是5字节（列如：0x00 0x05）。

在密钥衍生过程中使用的密钥：

— Ks（例如：CK‖IK连接）在第5.1节和第5.2节中说明，

注意：在本规范中，这个函数表示为：

Ks_NAF = KDF（Ks，“gba-me”，RAND，IMPI，NAF_Id），

Ks_ext_NAF = KDF（Ks，“gba-me”，RAND，IMPI，NAF_Id），

Ks_int_NAF = KDF（Ks，“gba-u”，RAND，IMPI，NAF_Id）。

标准分享网 www.bzfxw.com 免费下载

附 录 B
（资料性附录）
GBA 中，用户选择 UICC 应用的对话框实例

对于某种情况，5.1.4.8节描述了在GBA过程中用户是如何选择UICC应用的。一个对话窗口实例描述了这个过程，如下：

— 对话的标题："认证请求"。

— 解释："一个服务请求你去认证，请选择你的身份："

— 身份列表：UICC上的可选择的应用列表。每个应用的可见文本，是从UICC的应用列表的"标识"域中摘录出来的。

— 按钮："选择"和"取消"。

附 录 C
（规范性附录）
保护参考点 Zn/Zn′的 TLS 描述文件

本附录适用于使用DIAMETER或HTTP时的Zn′参考点，和使用HTTP时的Zn参考点。

TLS文件对密码包有如下限制，具体描述见RFC 3588：

BSF 和 Zn-Proxy 使用密码包 TLS_RSA_WITH_3DES_EDE_CBC_SHA 或 TLS_RSA_WITH_AES_128_CBC_SHA。

另外，Zn-Proxy证书，比如说，在TLS握手使用的客户端证书，应该包含RFC 3280里面介绍的subjectAltName扩展名。subjectAltName扩展名应该包含一个或者多个dNSName名。dNSName名可能包含通配符特征‘*’和RFC 28183.1部分描述的匹配需要被执行。

Zn-Proxy证书应该包含所有会通过Zn-Proxy向用户的归属BSF请求NAF相关共享秘密的NAF的NAF_ID。如果增加了新的NAF，则新的DNA名通过通配符标志方式隐藏在证书当中（例如：“*.operator.com”），或者证书中添加一个新的dNSName名。在后面的情况下，Zn-Proxy需要一个新的证书。

标准分享网 www.bzfxw.com 免费下载

附 录 D
（资料性附录）
TLS 证书的处理

存在TLS的认证架构。这个附录的目的就是为在TLS证书认证框架不存在的情况下，提供TLS证书在参考点Zn'上应用时的可选的指导方针。

本附录中，下面的缩写语要使用：CA_A是A网络中的证书权威机构，CA_B是B网络中的证书权威机构。$Cert_A$是A的证书，$Cert_B$是B的证书。I_A是A用来作为NAF_ID使用的标识符。T_B是B所信任的对等实体。

D.1 TLS证书注册

TLS的相互认证基于公钥技术和证书。TLS对等实体A和B应该包含一个证书存储，并且还应该有一个认证权威机构（CA），这个CA可以在包含A和B的安全域内发放证书。$Cert_A$ 包含A的标识符的I_A。每个标识符以正式域名（FQDN）的形式。同样的，B的证书是$Cert_B$ 。

B内存储的证书规定B所信任的对等实体的组T_B 。证书的创建与注册存在多种方式，下面描述了其中的3种。

a）第一种方式就是只有一个认证权威机构CA_B，并且这个权威机构存在于B的网络。CA_B 发放一个证书$Cert_B$给B，发放一个证书$Cert_A$给A。这些证书通过一种安全的方式（“out of band带外方式”）从CA_B传送到A和B。然后，A和B都通过将对等实体证书插入到他们的证书库里的方式，来将他们的对等实体添加到他们所信任的对等实体组里面：A插入$Cert_B$到A的证书库里，B插入$Cert_A$ 到B的证书库。这个插入过程是典型手动的，并且细节方面决定于证书存储管理接口的执行。

b）第二种方式，A和B的网络分别包含认证权威机构CA_B和CA_A 。CA_B发放$Cert_B$给B，CA_A 发放$Cert_A$给 A。证书通过一种安全的方式（“out of band”）从CA_B传送到A以及从CA_B发到 B。然后，A和B通过插入对等实体证书到证书库的方式将他们的对等实体添加到他们所信任的对等实体组里面，：A插入$Cert_B$到A的标识符存储，B插入$Cert_A$到B的标识符存储。

c）第三种方式，两边的CA证书相互交换：CA_B的证书以安全的方式（“out of band”）传送给A，CA_A的证书以安全的方式（“out of band”）传送给B，然后插入到证书库，并且标识为可信任的。TLS握手过程中，进行交换的$Cert_A$和$Cert_B$的确认基于证书库中存在的相关CA证书。

注意：在第一种方式和第二种方式中，如果对等实体可以产生标识自己的证书，并且可以以安全的方式（“out of band”）来进行交换，则可以不需要认证权威机构。在这些方式中，证书指纹可以代替证书本身来进行交换。

D.2 TLS证书撤销

在PKI—撤销接口不存在的情况下，证书的撤销需要手动执行。撤销操作包括将A从B所信任的对等实体组TB 中移除。对于上面所描述的前两种注册过程，证书的撤销需要B将A的证书（$Cert_A$）从证书库中移除。这个移除需要手动来完成。在第三种方式中，A的证书不在B的证书库里面。由于这个原因，B必须与A的证书的发送者一起，选择一种方式来检测证书A（$Cert_A$）的合法性（在前两种注册方式中，如果B和证书发放者一起能检测证书A的合法性，则手动维持操作量就可以减少）。这种检测可以通过在线证书状态协议（OCSP）来完成，或者通过$Cert_A$证书发放者公布的证书撤销列表（CRL）来完成。

附 录 E
（规范性附录）
GBA_U UICC-ME 接口

这个附录描述了在GBA自举过程中，当支持GBA_U的UICC应用被激活并且ME需要参与其过程时，使用的UICC-ME接口。当UICC应用不支持GBA_U时，ME在非GBA_U的安全上下文中使用AUTHENTICATE命令（例如：在USIM情况下，使用UMTS安全上下文，在ISIM情况下，使用IMS安全上下文），这些内容在TS 31.102和TS 31.103中有详细介绍。

E.1 GBA_U自举过程

这个过程是5.2.3.2节中描述的自举过程的一部分。

ME将RAND和AUTN发送到UICC，将按照5.2.3.2节描述的过程来生成Ks。

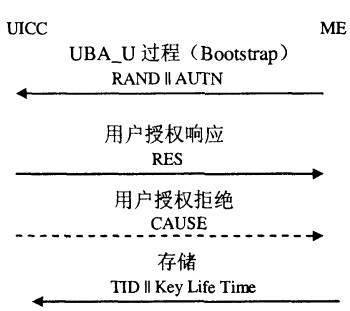
UICC储存Ks。UICC也储存使用过的RAND，用来确认当前建立的密钥值。ME也可以获得UICC中的RAND。

ME最后结束自举过程，并且将与以前建立的密钥相关的B-TID和密钥生命时间存入UICC。ME应该可以访问UICC中的B-TID和密钥生命时间值。

GBA_U自举过程的最后，UICC要存储Ks，B-TID，密钥生命时间和RAND。

UICC发送RES到 ME。

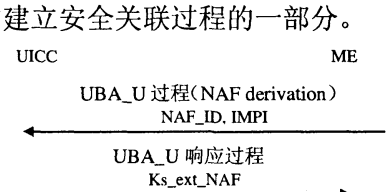
一个新的自举过程取代了前一个自举过程中的Ks，B-TID，密钥生命时间和RAND。



E.1 GBA_U建立过程

E.2 GBA_U NAF衍生过程

这个过程是使用5.2.3.3节描述的建立安全关联过程的一部分。



E.2 GBA_U NAF衍生过程

ME将NAF_ID和IMPI发送到UICC。UICC根据5.2.3.3节描述的过程来衍生Ks_ext_NAF和Ks_int_NAF。UICC使用上一次自举过程产生的RAND和Ks。UICC返回Ks_ext_NAF到ME，并且保存Ks_int_NAF和相关的B-TID，NAF_Id也与这两者一起保存。

标准分享网 www.bzfxw.com 免费下载

注：以前的GBA_U Bootstrap在前面的过程采用。如果UICC里面的Ks无效，则将会在命令中显示合适的错误信息。

输入的参数IMPI和作为NAF-ID一部分的FQDN利用UTF-8编码方式，编码成为一个字节串，参见IETF RFC 3629（2003）。

附 录 F
（资料性附录）
密钥对存储

F.1 介绍

与所请求的用户证书相关联的公/私密钥对的存储牵涉到用户证书的发放流程。

可以用不同的方法存储密钥对。这种存储的性质可能对与用户证书相关的信任水平产生影响。

本附录提供了不同场景下的密钥对存储的安全风险分析。

F.2 密钥对存储的应用场景

有不同存储与用户证书请求相关的公/私密钥对的场景。

F.2.1 在ME上存储密钥对

移动设备是存储密钥对的一个可能场所。

在ME上存储密钥对有2种选择：在MT上存储或者在TE上存储。

F.2.2 在UICC上存储密钥对

另外一种存储密钥对的方法是在UICC上存储。

在以下的研究中，将只考虑2种密钥对的存储场景：在ME 上存储或者在UICC上存储。

F.3 与密钥对相关的威胁

F.3.1 密钥对生成

就私钥的保密性而言，密钥对生成是一种非常敏感的操作。生成的密钥对必须有良好的质量，并且产生密钥对的设备和密钥对存储的设备之间的交互必须得到保护，以避免私钥克隆或泄漏。与ME相比，UICC可以提供更高级别的保护，以抵御对私钥的未经授权的访问。

F.3.2 对私钥的未授权使用

与对私钥的未授权使用相关的威胁有2种：

a）攻击者掌握私钥；

b）攻击者使用受害者的私钥却不掌握该私钥。

关于威胁a），在UICC中使用密钥可以比在ME中使用密钥提供更好的保护。然而，即使密钥在UICC中，能够破坏ME的攻击者也有可能使用密钥进行未授权的操作，因为UICC和用户之间没有直接的可信任路径。

由威胁b）造成的攻击通常要求与UE有互操作以进入UICC。但在威胁a）的场景下，密钥一旦被获取，相关的攻击就不要求与UE有任何互操作来使用所得到的私钥。

F.3.3 可移植性

如果密钥对存储在移动环境中，当一个新的UICC插入此ME时，就会产生一种威胁。在ME上存在不属于新用户的私人的和敏感的数据。由于对私钥的访问受到PIN或密码的保护，除非新用户知道PIN或密码，否则他不能访问私钥。

标准分享网 www.bzfxw.com 免费下载

另外，基于AKA的用户证书登记的一个重要方面是使用短期证书。在使用短期证书时，即使新用户能够访问老用户的私钥，在授权交易中，新用户也有可能无法假冒老用户，因为如果用户证书过期，新用户就得不到代表老用户的密钥对的用户证书。另外，如果ME中的密钥对是短期的，在密钥对过期后，新UICC的所有者就不能够使用该密钥对。但不能假设当新用户获得老用户的私钥时，用户证书/密钥对已经过期。通常说来，在UICC或者ME上的短期密钥对于身份和私密性保护很有作用。频繁地更换密钥对可以防止外来者把同一用户所做的交易联系在一起。

F.3.4 环境

对于密钥对的威胁取决于环境，即存储密钥对的地点。

所有在移动终端、PC、MAC或者PDA上面实现都会留下潜在的危险，比如有可能安装木马、蠕虫或者病毒。软件应用缺少智能卡中存在的保护机制（抗破坏、重要电路的物理封装）。逆向工程技术，比如提取程序码和拆分/调试手段，在软件环境中被极大地简化，使得令牌的秘密部件，比如密码运算、私钥和其他假设的安全信息，都被发现。

目前，在移动环境并不具有UICC中的所有的硬件或软件手段来对抗收入侵性和非入侵性的攻击，这些攻击是为了取得秘密。但是类似代码签名的机制已经得到了应用。

F.3.5 对于数字签名的必要属性的威胁

数字签名必须具备以下属性才可以有效：

— 真实性：有效的签名表示签名人有意在相关的信息上签名；

— 不可取代性：只有签名人可以为相关的信息提供有效的签名；

— 不可重用性：对一个文本的签名不能用于另一文本；

— 不可否认性：签名人不能否认已经在某个文本上作了有效签名；

— 完整性：保证内容没有被修改。

这些属性涉及到密钥资料的机密性，拥有到用户的可信的输入/输出路径，以及使用强大安全的密码机制。

因此，对于数字签名的信任取决于密钥对的存储和相关的密码计算，以及用户和执行私钥操作的模块之间的通信的安全性。在F.4节中将研究密钥对存储的影响。

F.4 与密钥对存储相关的安全风险分析

很多不同的用户应用场景描述了使用用户证书的应用或服务的范围。但是，与所推荐的服务相关的信任级别取决于密钥对的存储。以下的安全风险分析将对此加以介绍。

F.4.1 用户证书使用场景

用户证书的使用可以分为以下两大类。

F.4.1.1 安全服务

这些服务提供便捷的方法来认证cellular用户。这些服务可以由cellular运营商、企业或者第三方内容提供商提供。安全服务也可以支持付款。

不同的用户使用场景如下：

— 人对人的认证：一对一认证

— 企业服务：认证企业内部网的应用；

— 人对内容：

— 使用Presence服务；

— 自助服务管理；

— 使用运营商的Web服务；

— 使用第三方的内容服务；

— 加强的LCS私密性；

— 通过cellular网络通知；

— MBMS安全；

— 支持Liberty Alliance的应用场景；

— 通过cellular运营商进行小额到中额的付款。

F.4.1.2 安全连接

这种服务利用cellular基础设施和已存在的运营商-客户关系来认证用户：

— 可选的访问认证：

— 企业WLAN访问认证；

— 宽带访问，比如DSL 或光缆访问；

— 服务认证，比如VPN认证。

F.4.2 某些场景下的安全风险分析

所有的用户使用场景并不要求密钥对存储具有同样的安全级别，因为用户使用所需的服务具有不同的特点：

— 附加值：高或低附加值服务；

— 涉及到的伙伴和信任关系：在不同的cellular网络运营商，或者cellular网络运营商和服务供应商或者第三方内容供应商之间，存在协议；

— 所需证书的类型（短期证书或者长期证书）。

本节介绍了某些场景，其中的密钥对存储的性质对于服务的安全有影响。

F.4.2.1 涉及用户私人信息的场景

一个涉及用户信息场景的例子是自助服务管理。

F.4.2.1.1 自助服务管理

这种场景允许用户对运营商的Web 入口进行认证，以对self-provisioning进行安全访问。可以在终端和Web 入口之间建立安全的端对端（TLS）通道（以标准的方式使用用户的私钥和证书，即不需要改动TLS）。用户可以拥有移动或者固定的网络连接（比如GPRS，WLAN或者 xDSL）。主要的应用场景是付款信息查询和修改某人的注册资料。

用户经验：

授权可以直接基于用户证书，或者基于用户证书和Web 入口中的访问控制列表的联合认证。在第一种场景下，自助管理服务器：

— 接收到数据拥有者签名的声明，其中包括公钥和一系列访问权限；

— 验证声明发送人拥有相匹配的私钥；

— 只有验证成功才允许进行安全访问（比如TLS连接）。

F.4.2.1.2 在这种场景中的安全风险分析

标准分享网 www.bzfxw.com 免费下载

根据F.3.2节规定的非授权使用威胁来进行安全风险分析。

—— 未经授权就使用受害者的私钥，但是不获得私钥：

— 潜在的攻击：

攻击者可以使用用户私钥来认证Web 入口，并且访问self-provisioning。比如，攻击者可以修改用户的注册信息。

— 可行性：

攻击者需要与UE进行交互，以访问UICC。

这种攻击用于以下情形：

— 密钥对存储于ME上；

— 密钥对存储于UICC上；

—— 通过掌握私钥来进行未授权使用：

— 潜在的攻击：

攻击者可以使用用户私钥来认证Web 入口，并且访问self-provisioning。比如，攻击者可以修改用户的注册信息。

— 可行性：

一旦取得私钥，攻击者不需要与UE设备进行任何交互就可以访问UICC。

这种攻击用于以下情形：

密钥对存储于ME上：

这种攻击前提是取得密钥。由于UICC可以抗破坏，所以该攻击不能作用于UICC。

—— 这些攻击的后果：

自助管理是低附加值的，并且在UE上存储密钥对的后果是有限的。

F.4.2.2 涉及运营商和服务供应商间付款及协议的场景

有些场景涉及cellular网络运营商和服务供应商间的付款及协议。

F.4.2.2.1 通过cellular网络传送通知

用户授权服务供应商通过cellular网络传送通知。服务供应商不需要了解用户的身份。如果证书中没有身份信息，那么用户不用告诉服务供应商姓名。然而，用户可以通过电话支付通知的费用。用户授权此类付款，当服务供应上发出通知时，即开始计费。

—— 用户经验

在交易中，UE向服务供应商发出一个声明，即已签署的授权书，以便通过cellular网络、用户证书或者用户证书URL把通知信息传送给UE。服务供应商根据用户证书来验证授权文本和UE的签名。如果签名和授权文本都正确，服务供应商将把确认书发送给UE。

稍后，比如有某个体育赛事举办，服务供应商就起草一份通知，并把它连同已签署的UE授权书和用户证书发送给运营商。运营商验证已签署的授权书。如果验证成功，运营商将通过SMS或者MMS信息把通知文本发送给用户。

F.4.2.2.2 通过cellular运营商进行小额或者中额的付款

用户通过电话账单（或者通过独立的账单）授权对某项服务付款。注意服务供应商不需要了解用户的身份。如果证书中没有信息，用户就不需要把姓名告诉服务供应商。服务可能是，在某个non-cellular环境中，运营商传统的支付机制不能直接使用，也可能是non-cellular由第三方提供。

在支付交易中，UE把已签署的发票和用户证书（或用户证书URL）发送给服务供应商。服务供应商在用户证书的帮助下验证UE的签名。如果签名和发票都无误，服务供应商就允许UE使用所需的服务，或者发送所需的服务。

在清算阶段，服务供应商把已签署的发票发送给运营商以供验证。如果验证成功，运营商将偿还服务供应商，并通过用户的电话账单（或独立的账单）向用户索取服务费用。

—— 前提

服务供应商与发放用户证书的运营商有业务关系，并且知道运营商的签名验证密钥。

如果服务供应商（比如在国外访问的网络供应商）与用户的主网络没有直接关系，证书应该来自所访问的网络。独立的访问网络供应商信任所访问的运营商以及来自该运营商的用户认证书和证书。

—— 用户经验

用户信任来自主运营商的账单，并且付款方便。在使用服务时，他必须在付款中输入PIN来设定金额。终端可以自动签署很小的金额。在这种场景下，只有权限之上大笔金额和累计金额需要进行PIN询问。

F.4.2.2.3 这些场景中的安全风险分析

这些安全服务涉及付款以及cellular网络运营商和服务供应商之间的协议。密钥对存储的性质有一些后果。根据F.3.2节中确定的非授权使用威胁来执行安全风险分析。

—— 使用受害者的私钥来进行未授权操作，而不用取得私钥：

— 潜在的攻击：

如果 ME 不够安全，攻击者可以用一个程序来向用户显示某条信息（支付 1 欧元），但是要求 UICC 签署一条不同的信息（支付 100 欧元）。如果攻击者的程序破解了 PIN，在用户不知道的场景下，它就可以命令 UICC 生成签名。

— 可行性：

攻击者需要与 UE 交流来访问 UICC。

这些攻击存在于：

— 密钥对存储于 ME 上；

— 密钥对存储于 UICC 上。

—— 通过掌握私钥来进行未授权操作：

— 潜在的攻击：

如果攻击者设法破解了用户的私钥，在给服务供应商发送已签署的授权书时，攻击可能发生，那么用户就要支付他根本没有要求过的服务。

— 可行性：

一旦取得了密钥，攻击者不需要与 UE 设备进行任何交流就可以访问 UICC。

这种攻击存在于：

— 密钥对存储于 ME 上

标准分享网 www.bzfxw.com 免费下载

这种攻击的前提是取得密钥。由于 UICC 可以抵制篡改，所以该攻击并不会影响 UICC。

—— 这些攻击的后果：

— 可替代：用户可能要支付他未曾要求过的服务

— 否认：cellular 网络运营商和服务供应商尽管提供了服务，却拿不到报酬。

— 如果系统有可能受到攻击，签名人会否认所作出的签名，认为系统不安全。所以，在用户没有同意的场景下，如果有可能使用用户私钥，那么用户可以否认作出供认证的签名，并且不用支付相关的电话账单。

— 运营商和服务供应商尽管提供了服务，却拿不到报酬。

— 运营商和服务供应商之间的信任关系可能被破坏。服务供应商并没有安全担保，它将不再信任由 cellular 网络运营商发放的用户证书和相关的签名。

— 如果有些问题是由于未经授权就使用用户私钥造成的，那么对于 3G PKI 的信任可能会丧失。

— 涉及到付款和与服务供应商或第三方内容供应商关系的高附加值服务常常要求使用长期的证书。长期证书的发放比短期证书有更严格的安全要求。所以，根据 UE 上存在的未授权使用威胁，安全水平可能满足不了长期证书发放和使用的安全要求。

F.4.3 风险分析总结

为了防止确认的未授权使用私钥，需要给出以下建议：

— 以安全的方式存储私钥，并进行相关的密码运算；

— 解决办法宜提供使用私钥的安全路径。

在安全性方面，UICC提供最安全的存储和使用私钥的场所（比如以使用WIM的格式）。这并不排除对某些服务使用别的场所。另一方面，ME可以提供私用密钥的安全路径（比如通过密码签名的机制）。这些方法的结合将提供一个完整的安全的办法，来实现安全服务。

附 录 G
（资料性附录）
通过认证代理和 HTTPS 接入到应用服务器的技术方案

本附录将介绍认证代理技术，旨在引导认证网络部署。一个认证代理服务器担任着转换服务器的角色，使得来自于WEB服务器（AS）的网页（及其他内容）看上去像是源于此认证代理服务器。

为了描述多个不同DNS域名的host位于同一服务器（本例指代理服务器）的情形，引入了虚拟host的概念。

在运行HTTPS协议时的一种方案是给每个host关联不同的IP地址（基于IP的虚拟host）。这种方案的实现可以是一个主机采用多个物理网络连接的方式，也可以采用多个虚拟端口的形式，端口支持于常见的操作系统（常称为“ip 别名”）。这个方案采取每个应用服务器（AS）分配一个IP地址的方式，不允许“每UE到AP-NAF连接仅用一个TLS隧道”服务于NAF后面的所有应用的概念。

如果只想要一个IP地址，或想“一个TLS隧道通道”，就只能采用基于域名（name based）的虚拟host方案。考虑到HTTPS的使用，此方案会有问题，需要做适当调整才能工作。这种调整可能会致使代理服务器和浏览器偏离其标准行为。这种调整会涉及UE，且通常得不到浏览器的支持，可能会有互操作的问题。其他的调整方式则会约束此代理所附着的应用服务器的行为。

为了解决不同DNS域名的服务器共站于一个认证服务器（AP）情况下的虚拟host接入问题，可在握手过程中采用以下任一方案来标识host：

— RFC 3546定义了TLS的扩展。这个RFC支持UE在初始TLS握手消息中指示出欲联的虚拟机（参看5.3.1）。

— 另一个替代方法是给AP发送一个有多个标识的证书。证书中包含AP的标识和依赖于此AP的每个服务器的标识。这种证书的验证在RFC 2818中有规定。

运营商可选择以上任一方法来实现认证代理功能。

标准分享网 www.bzfxw.com 免费下载

附 录 H
（资料性附录）
UE 和应用服务器间基于证书的互认证向导

这一章解释如何利用用户证书来进行UE和应用服务器间基于证书的互认证。UE和应用服务器间基于证书的互认证应基于TLS，详见IETF RFC 2246和IETF RFC 3546。

当UE和应用服务器想要进行基于证书的互认证时，UE事先已经录用了一个用户证书，详见第6章。UE得到用户证书后可和AS建立一个TLS隧道，详见RFC 2246和RFC 3546。

AS可能会在TLS握手阶段发CertificateRequest消息告诉UE它支持基于证书的认证，详见IETF RFC 2246的7.4.4节。消息中包括证书类型列表和可接受的证书权威机构（certificate authorities）列表。如果用户的证书（即运营商的CA证书）权威机构在可接受的证书权威机构列表中，AS可能指示给UE说它支持基于证书的认证。

如果可接受的证书签发机构列表包括用户的证书签发机构，UE可继续基于证书的用户认证。实现方式是在TLS握手阶段通过Certificate消息发用户证书，详见IETF RFC 2246的7.4.6和7.4.2。如果可接受的证书签发机构列表不包括用户的证书签发机构，用户就应发不包含任何证书的Certificate消息。

注 1：由于用户证书的有效期短，用户证书的使用不需要AS与签发证书的PKI门户在线联络。

如果AS收到的Certificate消息不包含任何证书，AS可以采用2种方式进行TLS握手：

— 如果AS的安全策略强制要求基于证书的用户认证，AS应响应致命握手错误警告，IETF RFC 2246，或

— 如果AS安全策略不强制（可选）要求基于证书的用户认证，AS应继续TLS握手，详见IETF RFC 2246。

注 2：为了成功的用双向认证证书在UE和AS之间建立一个TLS隧道，UE必须在UE的证书库中有AS证书的根证书，同时AS必须在AS的证书库中有UE的用户证书（也就是运营商的CA证书）的根证书。根证书是证书链的根，建议在UE和AS中将其标为“可信任”。

注 3：为了能使用用户证书接入到访问网（visited network）的AS，需要AS具备用户归属运营商的CA证书，且此证书在访问网AS中标为“可信认”。与此相关的流程不属于本部分范畴。

附 录 I
（规范性附录）
2G GBA

本附录描述了 GBA 的可选应用，即允许使用 SIM 卡或者 UICC 上的 SIM。本部分所述过程称为 2G GBA。2G GBA 允许应用以一种更安全的方式接入，优于使用口令或者非增强的 GSM。本部分对还没有部署 USIM 的运营商有帮助。

I.1 参考模型

参考模型同5.1.1节描述。

I.2 网络元素

I.2.1 自举服务器功能（BSF）

通用自举服务功能（BSF）和UE应该利用2G AKA协议和TLS协议进行相互认证，并且建立会话密钥，这个密钥将会应用在UE和NAF之间。BSF通过利用附录A中的密钥衍生过程，来限制对于相关NAF的密钥资料的适用范围。密钥衍生过程在密钥资料的生存期内被多个NAF使用。根据BSF的当地策略来设置密钥资料的生存期。

BSF可以从HSS获得GBA的用户安全设置（GUSS）。

BSF应该能够从HSS发送的认证向量类型发现签约用户是2G还是3G用户。

BSF可以保持一个列表，这个列表可以标记分配的NAF到了哪个NAF组。这个列表用来选择在GUSS里面哪一个应用相关的USS对于某个NAF是有效的。

注 1：运营商分配NAF到NAF组。NAF组在HSS里面定义的，并且所有属于同一个运营商的BSF都是应该平等的。由于这些网络元素属于同一个运营商的网络，所以NAF组的定义不必在协议里标准化。

注 2：NAF组可能是“归属”和“拜访”的。它允许BSF对于同一个应用发送USS，对于不同的NAF（比如拜访网络和归属网络的）要带有不同的授权标记。在拜访网络里（比如说）的NAF只是显示那些被请求的应用，但是它并不知道用户归属网络的分组。

I.2.2 网络应用功能（NAF）

自举结束以后，UE和NAF可以运行一些应用相关协议，在这些协议里面，消息的认证都是基于在UE和BSF相互认证过程中所产生的会话密钥。

针对NAF的一些假设：

—— UE和NAF之间以前没有安全关联。

—— NAF应该能够定位并且能够与用户的BSF进行安全的通信。

—— NAF在应用相关协议的运行过程中，应该能够获得在UE和BSF之间建立的一个共享密钥资料。

—— NAF应该能够通过BSF从HSS获得一个或多个应用相关的USSs，也可以不获得任何USS。

—— NAF应该能够根据本地政策来设定共享密钥资料的本地有效情况。

—— NAF应该能够检测共享密钥资料的生存期和本地有效条件。

标准分享网 www.bzfxw.com 免费下载

—— NAF应对是否接受2G签约用户有一个本地策略。然而，SIM是否对特定的Ua应用允许使用决定于相关的Ua应用。如果对某一个Ua应用有TS规范，如对Presence有TS33.141。除非规范明确禁止SIM使用，那么就可以允许运营商对是否接受这个Ua应用配置BSF策略。

注：如果不采取附加的措施GBA不能保证密钥Ks（_int/ext）_NAF的刷新性，即不能保证密钥没有在以前的Ua协议的执行中使用过。UE和NAF可以采取以下附加的措施来保证GBA中的密钥的刷新性：

1 在衍生一个新的 Ks_NAF 之前，再执行一次 Ub 协议（产生一个新的 Ks）。

2. 存储以前用过的密钥 Ks（_int/ext）_NAF，或者相应的密钥标识符 B-TID，直到它们生存期满。

支持 Ua 协议的一个 UE 和一个 NAF，在需要的情况下，需要采取相应的措施来避免重放攻击，因为 Ua 协议在无连接运行中不能防止重放攻击。

I.2.2a Zn-Proxy

5.1.2.3节内容同样适用于此。

I.2.3 HSS

所有用户的安全设置（USS），即GUSS，存储在HSS里。

HSS的要求：

—— HSS能够提供GUSS的永久性存储。

—— GUSS应该以这样的方式来定义，即不同运营商对于标准的应用描述文件的交互是可能的。

—— GUSS应该以这样的方式来定义，即运营商应用相关和已经存在的应用描述文件的扩展不需要这些元素的标准化就可以支持。

—— GUSS应该包含应用相关USSs，这些USSs包含着与一个或者多个应用的认证和认证信息相关的参数，这些应用是由NAF发起的。任何其他类型的参数在应用相关USS里面是不允许的。

注 1：NAF可以从它的本地数据库中直接获得签约用户的描述文件数据。

注 2：一种从GUSS里临时取消特定应用USS的可能是，如果签约用户临时取消了业务，那么HSS可以临时把特定应用的USS从GUSS里移去。这种操作BSF的GUSS不改变，只有当现在自举会话超时会更新，或者当一个新的修改过的GUSS携带着AV从HSS里取出时建立了一个新的自举会话，那么原来的GUSS会被覆盖。

—— GUSS应该能够包括为BSF应用的参数：

— 签约用户衍生密钥生命周期；

— 可选地指示 GUSS 最近一次被 HSS 修改的时间的时间戳。

注 3：这些参数都是可选的，如果用户的GUSS里面不存在这些参数或者用户没有GUSS，那么BSF就可以利用在BSF本地策略中的缺省值，这个本地策略是由一个MNO自己定义的。

—— HSS应该能够分配应用相关的USS到NAF组。可能出现不同的USSs针对相同的应用，但针对不同NAF组的情况。GUSS中对于USS数目的限制依赖NAF组的业务。

— 对于某个应用，如果没有 NAF 组定义，那么对于每个应用至多有一个 USS 存储在 GUSS 里面。

— 对于某个应用，如果 NAF 组定义了，那么对于每个应用至多有一个 USS 和 NAF 组被存储在 GUSS 里面。

—— 在HSS中NAF组的定义和所有属于同一个运营商的BSF都应该是平等的。

— UICC 类型和密钥选择信息对 2G 签约用户不要求。2G GBA 认为是基于 ME 的。

I.2.4 UE

UE需要的功能为：

—— HTTP摘要AKA协议的支持；

—— TLS的支持；

—— 在自举使用SIM的能力；

—— 在ME上对Ua应用指示SIM是否在自举里允许使用的能力；

—— 从Kc，RAND，SRES和Ks-input中衍生新密钥资料用于Ua口协议的能力；

—— 对NAF特定应用协议的支持（见TS33.221例子）

一个支持2G GBA的UE应该也支持3G GBA_U（如5.2.2节所述）和3G GBA_ME过程（如5.1.5节所述）。

I.2.5 SLF

5.1.2.6节所述同样适用于此。

I.3 自举架构和参考点

I.3.1 Ub参考点

参考点Ub在UE和BSF之间。Ub接口提供UE和BSF之间的互认证。它允许UE基于2G AKA架构bootstrap会话密钥。

I.3.2 Ua参考点

Ua参考点携带应用协议，适用UE和BSF协商的密钥资料来保护，其密钥资料由Ub口协议运行得到。

I.3.3 Zh参考点

在BSF和HSS之间的参考点Zh允许BSF取得请求地认证信息和所有GBA用户安全设置。2G认证中心的接口是HSS内部的，它不需要作为这个架构的一部分被标准化。

I.3.4 Zn参考点

NAF使用Zn参考点取得前一次通过Ub口从UE到BSF密钥资料。如果NAF请求的话，从BSF在Zn口取得特定应用的用户安全设置。

I.3.5 Dz参考点

5.1.3.5节所述同样适用于此。

I.4 自举要求和原理

下面的原理与要求对于自举过程是适用的：

—— 自举功能不能依赖特定的NAF；

—— 实现自举功能的服务器需要被本地运营商所信任，才能去处理认证向量；

—— 实现NAF的服务器需要被本地运营商所信任，才能去处理衍生的密钥资料；

—— 在运营商的本地网络和拜访网络都需要支持NAF；

—— 这个架构不能排除在第三方网络中对网络应用功能的支持；

—— 已经存在的协议和基础设施需要得到最大限度的重新利用；

—— 为了确保最大限度的适用性，所有相关的协议都应运行在IP之上；

—— 要防止攻击者利用NAF的安全漏洞去成功的攻击其他的NAF，这里所涉及的NAF都使用GBA；

—— 要防止攻击者利用Ua口上一个安全协议存在的漏洞来实现对Ua口上另外的安全协议的成功攻击。

标准分享网 www.bzfxw.com 免费下载

—— 现存的SIM卡和UICC上的SIM和它们的规范应该不被影响。

—— 如果USIM和ISIM存在，那么应按照第5章所述使用，并且不应使用2G GBA。

—— 如第5章所述，2G GBA不能影响基于GBA的USIM/ISIM。

—— 2G GBA不能降低USIM/ISIM用户的安全。

—— 2G GBA应将对基于第5章GBA的USIM/ISIM的改变最小化。

—— 2G GBA应该提供减轻可知GSM弱点的措施。

I.4.1 接入独立

自举过程是接入独立的。自举过程需要从UE的IP连接。

I.4.2 认证方法

UE和BSF之间的认证不能离开有效的蜂窝签约用户。认证应该基于GSM认证（称为2G AKA）协议。另外，BSF认证应该通过服务器证书基于TLS。

I.4.3 漫游

5.1.4.3节所述同样适用于此。

I.4.4 Ub参考点要求

参考点Ub的要求：

—— BSF应该能够认证UE；

—— BSF和UE应该能够基于I.4.2节所述进行双向认证；

—— BSF应该能够发送自举事务标识符到UE；

—— UE和BSF应该建立共享密钥；

—— BSF能够通知UE密钥资料的生存期；BSF通过Ub发送的密钥生存期将会指示生存期满。

注：这并不能排除UE根据UE的本地策略在生存期满之前刷新密钥。

I.4.5 Zh参考点要求

参考点Zh的要求：

—— 相互认证，可以提供保密性和完整性；

注 1：如果BSF和HSS都在同一个运营商的网络，这个要求可以通过物理或者专有的安全方式来满足。

—— BSF应该能够发送用户的自举信息请求；

—— 可选地，BSF可以有能力给HSS发送签约用户GUSS的时间戳（时间戳选项）；

—— HSS应该能够向BSF一次发送一个2G AKA鉴权向量；

—— HSS应该能够根据安全目的的需要向BSF发送完全的签约用户的GUSS。可选地，HSS可以有能力指示BSF，BSF是否已经有了基于GUSS时间戳的最近一次的GUSS拷贝（时间戳选项）。

注 2：如果用户的GUSS在HSS进行了更新，更新的GUSS不会立即传送到BSF。作为自举过程的一部分，当BSF下次通过Zh从HSS获取认证向量和GUSS的时候，BSF中的GUSS会被更新。

—— 没有与自举相关的状态信息需要在HSS保存；

—— 通过参考点Zh的所有过程都是由BSF初始化的；

—— 与HSS的不同接口的数目应该保持最少。

I.4.6 Zn参考点要求

参考点Zn的要求：

—— 相互认证，可以提供保密性和完整性；

—— 如果BSF和NAF在同一个运营商的网络内，基于参考点Zn的DIAMETER协议应该根据NDS/IP受到保护；

—— 如果BSF和NAF不在同一个运营商的网络内，在Zn-Proxy和BSF之间的基于参考点Zn′的DIAMETER应该利用RFC 2246中的TLS来保证安全；

注1a：附录D详细说明了TLS描述文件。

—— 基于Zn/Zn′接口的HTTP协议应该使用RFC 2246中的TLS来保护。

注 1b：附录D详细说明了TLS描述文件。

—— BSF应该保证发出请求的NAF能够被批准去获得密钥资料和请求的USS；

—— NAF应该能够发送密钥资料请求到BSF，BSF 包含着UE相关请求使用的NAF的公共主机名。BSF应该能够保证NAF可以获得批准去使用这个主机名，比如说，UE与NAF通信时使用FQDN；

—— BSF应该能够发送密钥资料到NAF；

—— NAF应该能够从BSF中有选择性的获得应用相关的USS，NAF能够获得什么USS决定于BSF的策略和NAF通过参考点Zn的请求消息中的指示；

—— NAF应该能够向BSF指示出它所需要的USS用于一个或者多个应用；

注 2：如果某些应用只需要特定应用USS的子集，那么NAF从BSF的全部USS选择这个子集。

—— 如果私人签约用户信息和特定应用的USS发送到NAF，那么BSF应该能够基于每一个NAF或者每一个应用进行配置。

注 3：当需要决定使用哪种用户身份发送给NAF时需要考虑到隐私问题。如果希望服务连续性，那么BSF可以配制成发送IMPI（但是没有用户假名）。如果BSF不在USS里发送IMPI、IMPU或者假名，那么UE对于NAF是保持匿名的，或者更准确地说，B-TID是作为一个临时用户标识的。这可以引起NAF不能提供服务的连续性，因为当UE使用一个新的B-TID进行自举并联系NAF时，NAF需要用户身份来为Ua会话更新密钥。如果需要用户身份，NAF可以请求USS，BSF可以配制成在USS里发送用户假名，而不是IMPI。

—— 如果一个NAF向BSF请求USS，但是用户的GUSS里面不存在USS，倘若BSF本地策略的条件满足了，这就不会引起一个错误。BSF应该仅将要求并找到的USS发送给NAF；

—— 按照下面的描述来配置一个本地策略是可能的：对于一个相关请求的NAF，BSF可能需要一个或者多个应用相关的USS在这个用户相关的GUSS中，如果条件没有满足，就要拒绝来自NAF的请求。为了满足这个本地策略，NAF不需要通过Zn 参考点来请求USS，这些USS是BSF要求在GUSS里面存在的，只需要BSF在本地查询USS就已经足够了。在发出请求的NAF没有要求USS的情况下，配置BSF也是可能的；

—— BSF应该能够向NAF指示出自举的时间和密钥资料的生存期。BSF通过Zn传递的密钥生存期，应该与BSF通过Ub传递给UE的密钥资料的生存期一样。

注 4：这并不排除NAF根据本地策略在密钥过期之前更新密钥。

注 5：如果一个或者多个传送到NAF的USS在HSS的签约用户的GUSS里被更新，那么这个改变要继承到下次NAF通过Zn口从BSF得到USS时（提供BSF已经在Zh口从HSS更新了签约用户的GUSS）。

—— BSF应该发送消息给NAF，签约用户是2G用户。如果没有类似的信息发送，那么NAF应该假设用户是3G用户。

标准分享网 www.bzfxw.com 免费下载

注 6：这个请求使得NAF可以根据本地策略接受2G签约用户。第二句话保证了本部分第5章过程的后向兼容性。注意到GUSS里签约用户类型包含的信息不能够满足这个要求，因为GUSS不需要呈现给每个签约用户。

—— BSF可以根据本地策略决定NAF是否给2G用户提供服务。如果是这样的话，BSF不发送密钥给NAF。

注 7：这个要求允许运营商来控制BSF决定哪一个应用应该只使用3G安全。这个请求对那些无法估计BSF发送的签约信息类型的NAF也有必要，如Rel 7以前的NAF。

—— NAF应该能够指示BSF，Ua安全协议的协议标识，以及通过BSF发送的NAF-ID请求的密钥资料。

I.4.7 自举事务标识要求

Bootsrapping事务标识（B-TID）通过参考点Ua ，Ub和Zn将用户身份和密钥资料绑定。

B-TID的要求：

—— B-TID应该是全局唯一的；

—— B-TID应该作为一个密钥标识符来使用，应用在Ua 参考点上；

—— NAF应该能够从B-TID中检测到UE的归属网络及相应的BSF。

注 1：NAF在密钥无效之后，要删除那些符合删除条件的安全关联。

注 2：UE和NAF之间使用GBA还是非GBA认证，不能产生冲突，比如说在同一个命名空间。这种潜在的冲突不能通过通用的方式来解决，因为它依赖于相关的协议和UE与NAF之间所使用的认证机制。这超出了本规范的范围。

对于在UE和NAF之间使用的HTTP摘要认证的例子，下面的这种使用方式也是可能的：〈用户名，密码〉对在一个域内必须是唯一的。由于NAF控制域名，所以它必须确保只有基于域的GBA才能以保留的3GPP域名来进行命名。在特殊的情况下，NAF 要在GBA域内允许基于非 GBA的认证，它必须确保没有基于GBA认证之外的用户使用B-TID格式的用户名。

I.4.8 UICC和SIM卡选择要求

如果在UE里有UICC，包括USIM或者ISIM。那么如5.1.4.8节所述应该使用USIM或ISIM。否则，使用SIM。

如果没有UICC，但是UE里有SIM卡，那么使用SIM卡。如5.1.4.8所述，从IMSI得到IMPI。

I.4.9 Ua参考点要求

5.1.4.9节所述同样适用于此，并且：

—— 2G GBA的ME（也支持3G GBA）应在应用请求消息里指示给NAF签约用户的类型，特别是当用户是2G签约用户时。

—— NAF应在自举初始消息里指示UE其是否接受2G签约用户。

I.4.10 Dz参考点要求

5.1.4.10节所述同样适用于此。

I.5 过程

本节详细描述了为不同应用的2G GBA自举的过程。其过程包括与BSF的认证过程及密钥资料产生过程。

I.5.1 自举的发起

在UE和NAF进行通信之前，UE和NAF首先需要协商是否需要使用GBA。当UE要与NAF 进行通信，但是UE不知道NAF是否需要通过GBA方式产生共享密钥时，UE就需要进一步与NAF交互获取指示。

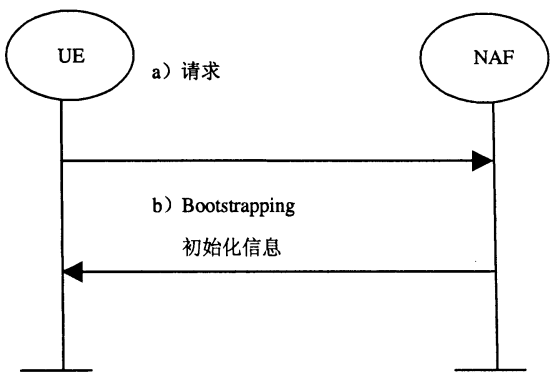


图 I.1　自举的发起

a）UE通过Ua参考点发起与NAF的通信。

b）如果NAF 需要使用通过GBA方式产生的共享密钥，但是来自UE的请求并不包括有关GBA信息时，NAF 回复一个自举初始化信息。这种通知的方式取决于相关的参考点 Ua，在相关的实现规范中详细说明。

如果2G SIM卡用户所访问的NAF并不支持2G GBA，为了避免浪费AV及网络资源，存在如下可选解决方案：

如果UE和NAF采用HTTP digest认证，那么UE可以在向NAF发送的http请求消息里的“user agent”头中包含一个“product”值。如果UE使用的是2G GBA密钥（即2G用户），那么该值设为“3GPP-gba-2G”和“3GPP-gba”2个值。如果NAF不识别“3GPP-gba-2G”，那么会自动放弃这条消息，只识别可以识别的“3GPP-gba”。

如果UE和NAF之间采用PSK TLS认证方式，那么可以通过设置“ServerKeyExchange”消息里的psk_identity_hint 的值来表示，即 psk_identity_hint 的值要同时包含“3GPP-bootstrapping-2G@naf.operator.com”和“3GPP-bootstrapping@naf.operator.com”（假设NAF域名是naf.operator.com）。

如果UE和NAF采用HTTP digest认证，那么NAF可以在向UE响应的“401 Unauthorized response”消息里通过设置 realm 的值来表示：如果 NAF 支持 2G GBA，那么该值前半部分设为“3GPP-bootstrapping-2G”，后半部分是NAF域名。（如realm值可为“3GPP-bootstrapping @naf.home1.net”）；如果realm值没有字符串“3GPP-bootstrapping-2G@naf.home1.net”，则表示NAF不能为2G用户服务。

如果UE和NAF之间采用PSK TLS认证方式，那么NAF可以在向UE响应的“ServerKeyExchange”消息里通过设置 psk_identity_hint 的值来表示，即 psk_identity_hint 的值可以包含“3GPP-bootstrapping-2G@naf.operator.com”以及“3GPP-bootstrapping@naf.operator.com”的任一个或者2个（假设NAF域名是naf.operator.com）。

注：使用此方案，GAA客户端需要向GAA服务器询问2G flag。

编者注：1、本方案节约了AV的使用，并优化了Zn接口，但会增加Ua口的复杂度；2、有可能存在Ua口泄漏用户2G身份的风险。

I.5.2　自举过程

标准分享网 www.bzfxw.com 免费下载

UE与NAF通信，并且知道需要一个自举过程，那么它将首先进行自举认证。另外，只有当UE接收到NAF发送回来的自举初始化消息或者来自NAF的自举协商指示后，再或者当UE中的密钥生存期满的时候，才执行自举认证。

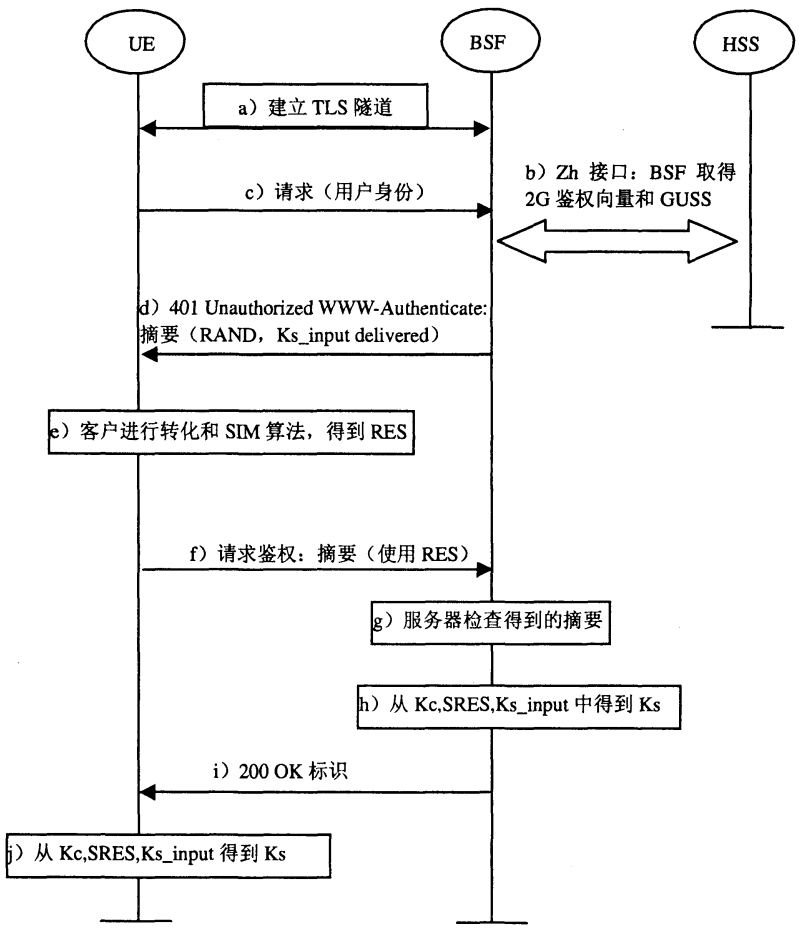


图 I.2　自举过程

a）UE与BSF建立一个机密保护的TLS隧道。在建立TLS隧道时，UE应使用BSF提供的证书对BSF进行认证。UE应检查BSF在证书里的“realm”值包含相同的BSF的FQDN。后续所有ME与BSF的通信都通过这个TLS隧道。UE现在发送初始HTTPS请求。

b）BSF通过Zh向HSS请求认证向量和GUSS。HSS通过Zh返回全部的GUSS和一个2G认证向量（AV=RAND，SRES，Kc）。BSF通过认证向量类型发现UE是2G SIM。

如果 BSF 在上一次自举过程应用时间戳选项，并且有从 HSS 得到的签约用户的本地 GUSS 的拷贝，这个 GUSS 包括时间戳，那么 BSF 可以在请求信息里包括 GUSS 时间戳。得到时间戳后，如果 HSS 应用时间戳选项，那么 HSS 将它与储存在 HSS 里的 GUSS 时间戳比较。在这种情况下，当且仅当 HSS 作了比较并且时间戳相等时，HSS 将“GUSS 时间戳相等”指示发送给 BSF。在其他情况下，HSS 把 GUSS（如果存在）发送给 BSF。如果 BSF 接收到“GUSS 时间戳相等”指示，它就存储 GUSS 的本地拷贝。其他情况，BSF 删除 GUSS 的本地拷贝，并且存储得到的 GUSS（如果发送）。

BSF将一个2G认证向量（RAND，SRES，Kc）转化成RES参数。

— RES=KDF（key，“3gpp-gba-res”，SRES），截得128位，key=Kc||Kc||RAND，KDF是密钥衍生函数，如附录A所述。

BSF还应选择一个128位的随机数“Ks-input”，并且设置服务器特定数据=Ks-input在HTTP摘要AKA里的aka-nonce里。

注 1：“截取到128位”的意思是从KDF256位的输出里，使用序号[0]到[127]的128位。

注 2：在多个HSS环境中，优先于步骤b），BSF可以通过询问SLF得到储存用户签约的HSS地址。

c）BSF应发送RAND和服务器特定数据在401消息里到UE（不包括RES）。这是命令UE认证BSF。

d）UE从消息里得到RAND，计算相应的Kc和SRES。它根据步骤b）的值计算出参数RES。

e）UE发送另一个HTTP消息，包括摘要AKA响应（利用RES计算出的口令）和一个cnonce给BSF。

f）BSF通过检查摘要AKA响应认证UE。如果认证失败，BSF不能在以后任何通信中使用此认证向量。

注 3：在“AKAv1”中的HTTP摘要AKA的密码是二进制。

g）BSF应计算密钥资料Ks，Ks=KDF（key，Ks-input，“3gpp-gba-ks”，SRES）. 通过对步骤c）里的RAND值进行base64编码，并与BSF服务器名共同编码，以NAI的格式来产生B-TID值，即，base64encode（RAND）@BSF_servers_domain_name。

h）BSF应该发送200 OK消息给UE，包括B-TID和authentication-info头，来指示认证成功。另外，在200 OK消息里，BSF应该提供Ks的密钥生命周期。

i）如果服务器认证失败，BSF应终止过程。如果成功，UE应按照与BSF相同的方法生成密钥资料Ks。

j）UE和BSF应该利用Ks产生密钥资料Ks_NAF。利用Ks_NAF来保证参考点Ua的安全。

Ks_NAF根据下面的公式来计算Ks_NAF = KDF（Ks，“gba-me"，RAND，IMPI，NAF_Id），KDF是在附录中说明的密钥衍生函数，密钥衍生参数由用户的IMPI，NAF_Id 和 RAND组成。NAF_Id的结构是：NAF_Id=NAF的FQDN||Ua安全协议标识。KDF也应该在ME内执行。

注 4：如果一个NAF拥有有相同FQDN和Ua安全协议标识的2个或多个应用，那么它们应共享相同的NAF衍生密钥。这会引起所谓的“two-time pad”，会导致这些应用的安全妥协的情况。这可以通过分别进行自举过程或者应用的特定方法避免，这超出了本标准范围。

在UE和BSF里要保持基于NAF名的一致密钥衍生，至少应该满足以下几个前提条件：

（1）在DNS内，NAF只有一个域名。比如说，不能存在两个不同的域名对应同一个NAF的IP地址。这要通过管理方式才能完成。

（2）NAF的每个DNS入口对应着不同的IP地址。NAF向所有的IP地址作出响应。每个IP地址通过NAF配置绑定到相应的FQDN。FQDN使用从IP地址中推出的NAF进行密钥衍生。

（3）Ua使用传输主机名（UE使用的NAF的FQDN）到NAF的协议（例如带有强制主机请求头域的HTTP/1.1）。这需要NAF检查主机名的有效性，从而在与UE所有的通信过程中都使用这个名字，还要将这个名字传送给BSF，达到正确衍生出Ks_NAF的目的。

在TLS隧道的情况下，这需要多身份证书或RFC 3546或者其他的协议的配置，但都是为了相同的目的。

UE和BSF将会存储密钥Ks和与其相关的B-TID，直到Ks的生存期满，或者密钥Ks被更新了，或者删除条件满足时。

I.5.3 使用自举安全关联的过程

在UE和NAF进行通信之前，UE和NAF首先必须协商是否使用以GBA方式产生的共享密钥。如果UE不知道与NAF是否使用GBA，它就需要使用在前面章节中描述的自举初始化过程。

一旦UE和NAF使用GBA建立了联系，UE与NAF每次交互都需要执行图I.1描述的几步。

标准分享网 www.bzfxw.com 免费下载

a）UE 通过参考点 Ua 向 NAF 发起通信：

对 I.5.1 描述的问题可以通过设置“3gpp-bootstrapping-2g” 标识来解决，

对此，特提出 2G 身份标识的可选解决方案：

如果 UE 和 NAF 采用 HTTP digest 认证，那么 UE 可以在向 NAF 发送的 http 请求消息里，通过使“user agent”头包含一个 “product”值来表示：如果 UE 使用的是 2G GBA 密钥（即 2G 用户），那么该值设为“3GPP-gba-2G”和“3GPP-gba”2 个值。如果 NAF 不识别“3GPP-gba-2G”，那么会自动放弃这条消息，只识别可以识别的“3GPP-gba”。

如果 UE 和 NAF 之间采用 PSK TLS 认证方式，那么可以通过设置“ServerKeyExchange”消息里的 psk_identity_hint 的值来表示，即 psk_identity_hint 的值要同时包含 3GPP-bootstrapping-2G@naf.operator.com 和“3GPP-bootstrapping@naf.operator.com”（假设 NAF 域名是 naf.operator.com）。

注：使用此方案，GAA客户端需要向GAA服务器询问2G flag。

编者注：1、本方案节约了 AV 的使用，并优化了 Zn 接口，但会增加 Ua 口的复杂度；2、有可能存在泄漏用户 2G 身份的风险。

—— 一般情况下，UE 和 NAF 还没有共享需要保护参考点 Ua 的密钥。如果已经共享了这个密钥（Ks_NAF 对于相关的密钥衍生参数已经是有效的），UE 和 NAF 就可以立刻进行安全的通信。如果 UE 和 NAF 还没有共享这个密钥，UE 就需要执行以下步骤：

—如果 UE 对于选择的 UICC 应用的密钥 Ks 是有效的，UE 就可以根据 Ks 衍生出密钥 Ks_NAF。

—如果 UE 内对于选择的 UICC 应用的密钥 Ks 是无效的，UE 首先要先与 BSF 通过参考点 Ub 协商一个密钥 Ks，然后进行衍生 Ks_NAF 的过程。

对于UICC应用，如果UE不想根据同一个密钥衍生多个Ks_NAF，UE就应该先与BSF通过参考点Ub协商一个新的密钥Ks，然后进行衍生Ks_NAF的过程。

—— 如果 NAF 与 UE 共享一个密钥，但是 NAF 要去更新这个密钥。比如说，这个密钥的生存期满或者马上到期，再或者这个密钥不能满足 NAF 本地有效条件，它就需要发送一个合适的自举重协商请求到 UE。如果密钥的生存期满，运行在上面的协议将会终止。这种通知的方式决定于运行在上面的协议。如果 UE 接收到自举重认证请求，它将会按照 I.5.2 节说明的方式执行，目的是获得一个新的密钥 Ks。

考虑到在UE和BSF内衍生密钥的一致性，两者都需要使用相同的FQDN进行衍生。运行在Ua上的协议都需要是指定在下列情况：只有I.5.2节的注1和注2被允许用于NAF，或者当Ua口使用的协议从UE到NAF传输用于产生衍生密钥的FQDN时。

注 1：如果在UE和NAF之间的共享密钥无效了，NAF就可以为后来的删除设置相关安全关联的删除条件。

—— UE 以 I.3.2 节中描述的方式把 B-TID 发送给 NAF，这样可以使 NAF 从 BSF 内获得相关的密钥。

注 2：UE 可以根据参考点Ua的特殊需要来调整密钥资料Ks_NAF。这种调整超出了本规范的内容。

——在 ME 里 GBA 相关密钥的密钥管理（即 Ks 和 Ks_NAF）在 5.1.4.11 节描述。

——当通过参考点 Ub 协商出新的密钥 Ks，NAF_Id 产生的密钥 Ks_NAF 被更新时，存储在 UE 内由与这个 NAF_Id 不同的 NAF_Id 产生的 Ks_NAF 将不会受到影响。

对于每个NAF-Id，UE内至多存储一个与之相对应的Ks_NAF。

b）NAF向BSF发送密钥请求消息，消息携带B-TID。

—— NAF根据通过Ua口UE提供的B-TID请求相应的密钥资料；

—— NAF还可以为应用请求一个或多个特定应用的USS，通过Ua口从UE接收的请求可以接入；

注 3：如果NAF要求服务连续性，那么NAF可以根据BSF策略请求一个包含用户假名可以允许服务连续性的USS。

—— 随着密钥资料请求，NAF应该提供NAF-Id（其包括UE用来接入这个NAF的FQDN和Ua安全协议标识）给BSF。（这样是为了以下步骤BSF和UE密钥衍生的连续性）。BSF应该能够确认NAF有权使用这个FQDN。

c)BSF 根据密钥 Ks 和密钥衍生参数衍生出密钥，该密钥用于保护参考点 Ua 上使用的协议（在 5.1.3.2 节里有详细说明）。然后将 Ks_NAF，自举时间，密钥的生存期和 GBA 类型发送给 NAF。如果在用户 GUSS 里面存在可以使用的 USS，并且这个 NAF 有权获得所请求的 USS，则 BSF 也将所请求的应用相关的以及潜在的 NAF 组相关的 USS 与 Ks_NAF 一起发送到 NAF。对于任意包含 NAF 组特征的 USS，这个特征应在提供给 NAF 时在 USS 里删除。BSF 应指示 NAF 此签约用户为 2G 用户。如果 NAF 所提供的由 B-TID 所标识的密钥在 BSF 里面无效，则在对 NAF 的响应消息里通知 NAF。NAF 将会向 UE 发起一个自举重认证请求。

—— NAF根据通过Ua口UE提供的B-TID请求相应的密钥资料；

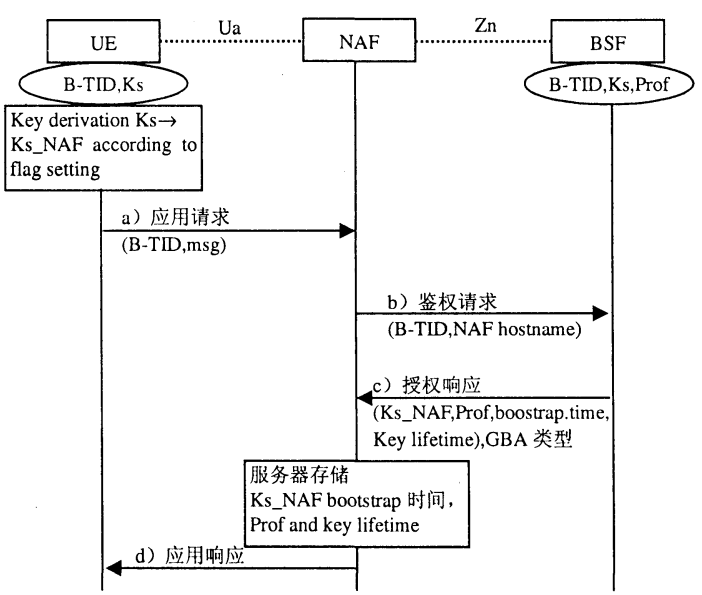
—— NAF还可以为应用请求一个或多个特定应用的USS，通过Ua口从UE接收的请求可以接入；

—— 随着密钥资料请求，NAF应该提供NAF-Id（其包括UE用来接入这个NAF的FQDN和Ua安全协议标识）给BSF。（这样是为了以下步骤BSF和UE密钥衍生的连续性）。BSF应该能够确认NAF有权使用这个FQDN。

d)BSF 根据密钥 Ks 和密钥衍生参数衍生出密钥，该密钥用于保护参考点 Ua 上使用的协议（在 I.5.2 节里有详细说明）。然后将 Ks_NAF，自举时间，密钥的生存期和 GBA 类型发送给 NAF。如果在用户 GUSS 里面存在可以使用的 USS，并且这个 NAF 有权获得所请求的 USS，则 BSF 也将所请求的应用相关的以及潜在的 NAF 组相关的 USS 与 Ks_NAF 一起发送到 NAF。另外，BSF 应该指示 NAF，签约用户是一个 2G 用户。如果在 BSF，NAF 提供的由 B-TID 标识的密钥不存在，那么 BSF 应在响应里对 NAF 指示此情况。然后 NAF 给 UE 指示一个自举重协商过程。

注 4：NAF可以根据本地策略，来设置Ks_NAF的本地有效条件。比如说，限制Ks_NAF重利用次数。

注 5：NAF将使用与UE同样的方式来调整Ks_NAF去适应参考点Ua的相关要求。该调整超出了本部分的范围。



msg is appl.specific dataset
Prof is application specific part of user profile

图 I.3 自举应用过程

标准分享网 www.bzfxw.com 免费下载

——BSF 可能要求在用户的 GUSS 内对应某个 NAF 必须存在的一个或多个与应用相关并且与潜在的 NAF 组相关的 USS。如果 GUSS 缺少一些要求的设置，则 BSF 就需要在向 NAF 响应中指出这一点。

——BSF 还可能根据 BSF 的策略将私人用户标识（IMPI）和所请求的 USS 发送给 NAF。

——如果根据本地策略，BSF 或者 NAF 决定，NAF 不给 2G 签约用户提供服务，那么 NAF 应该终止参考点 Ua 上的协议。

d）NAF 通过参考点 Ua 上的协议继续与 UE 进行交互。

一旦运行在参考点 Ua 上的协议完成，就达到了自举的目的，因为这能够使得 UE 和 NAF 在参考点 Ua 上安全的进行通信。

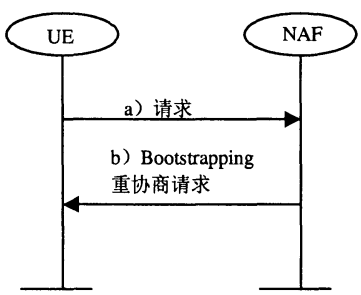


图 I.4　自举重认证请求

I.5.4　有关服务发现过程

UE应该从SIM上IMSI发现BSF的地址。5.1.5.4节所述同样适用于此。

I.6　TLS文件

UE和BSF应该支持RFC 2246和WAP-219-TLS所述的TLS版本，或者更高。不允许更早的版本。

注 1：根证书的管理超出了本部分范围。

注 2：证书撤销超出了本部分范围。然而，为BSF的证书选择短的生命周期可以降低风险，这样，BSF证书可以做出让步。

I.6.1　保护机制

UE 应使用密码包 TLS_RSA_WITH_3DES_EDE_CBC_SHA 或者 TLS_RSA_WITH_AES_128_CBC_SHA。

BSF 应支持密码包 TLS_RSA_WITH_3DES_EDE_CBC_SHA 和 TLS_RSA_WITH_AES_128_CBC_SHA。

I.6.2　BSF认证

客户应根据WAP-219-TLS所述对BSF进行认证，也可基于RFC 2246。

BSF证书文件应根据WAP 211 WAPCert基于WAP证书和CRL文件。

I.6.3　UE认证

BSF不应从UE在服务器Hello消息里请求一个证书。BSF应根据I.5.2对UE进行认证。

I.6.4　安全参数的建立

TLS握手协议协商一个会话，由会话ID标识。客户和BSF应允许重用一个会话。会话ID的生命期由UE和BSF的本地策略决定。建议生命周期为5min。最大生命周期为24h。

注：如果BSF坚持建议的生命周期，那么UE在自举重协商里能够重用TLS会话。

附 录 J
（资料性附录）
具备 GBA 功能的漫游用户访问漫游网络的 GAA 应用

J.1 概述

如果一个具备GBA功能的UE所在的归属网络不支持GAA，而当该UE漫游到一个支持GAA的漫游网络时，按照目前提供的通用认证架构和通过该通用认证架构访问NAF的处理方法，由于与用户进行互认证的BSF是归属网络的BSF，而该UE所属归属网络不支持GAA。因此，该UE是不能使用漫游网络提供的NAF业务的。

本节旨在探讨漫游用户具备GBA功能，该漫游用户所属归属网络不支持通用认证框架（GAA），而该漫游用户所处漫游网络支持GAA的情况。

J.2 GAA漫游的讨论总结

关于 BSF 寻址，根据现有规范，BSF 的地址是根据用户的 IMPI 中的 mnc 和 mcc 组成得到（参见 TS23.003 BSF addressing），即用户找到的 BSF 地址缺省回到其自己的归属网络。

如果根据运营商的大区建设原则，一个大区只有几个 BSF，是存在问题的。

针对此，可以采用：1）预置 BSF 地址的方式；2）采用 OTA 的方式解决；3）用户得到的不同的 BSF 域名可以映射到同一个 BSF 的 IP 地址，通过 DNS 的配置来解决。

标准分享网 www.bzfxw.com 免费下载

附 录 K
（资料性附录）
终端分离情况下的通用认证解决方案

K.1 终端分离情况下的通用认证框架解决方案—设备标志（Device-ID）方案

K.1.1 设备标志（Device-ID）方案

UE与NAF通信，并且知道需要一个自举过程，那么它将首先进行自举认证。另外，只有当UE接收到NAF发送回来的自举初始化消息或者来自NAF的自举协商指示后，再或者当UE中的密钥生存期满的时候，才执行自举认证。

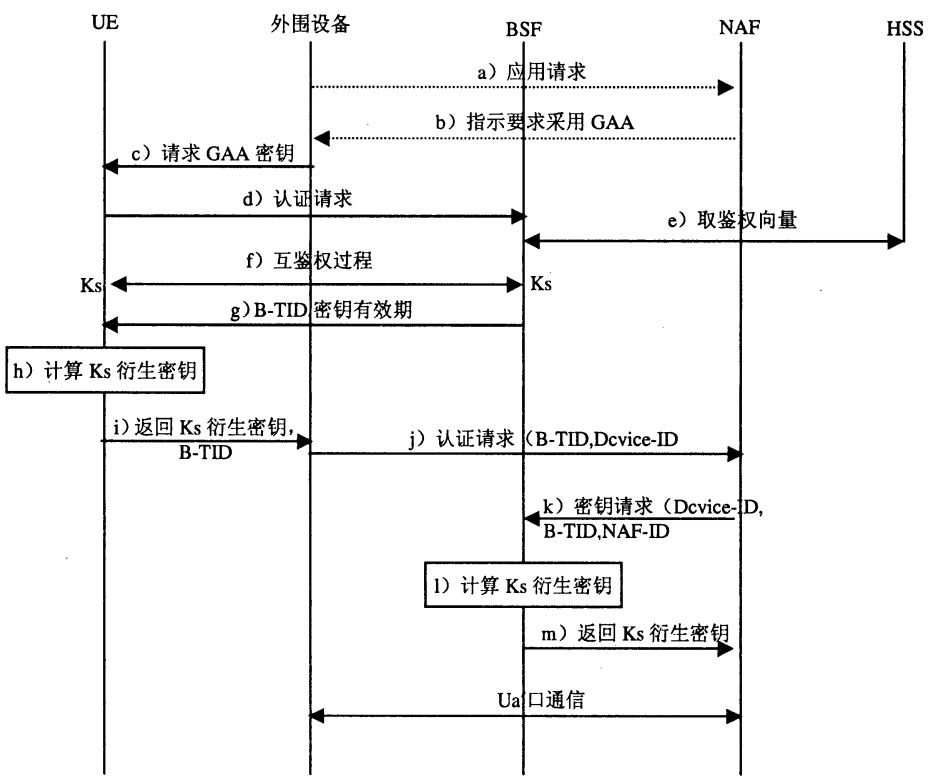


图 K.1 存在外围终端设备的自举过程及建立安全关联过程

a）外围终端设备上的NAF应用客户端向NAF发送请求，如果客户端本身知道NAF要求采用GAA密钥进行认证，就跳过这一步骤，直接进入步骤c）。

b）NAF查找该用户是否已经具备有效的密钥。如果没有，指示应用客户端采用GAA密钥与其进行安全通信。

c）外围设备上NAF应用客户端向UE请求NAF衍生密钥，并在请求消息里携带应用标识NAF-ID，自身设备标志。这里，设备标志是指用于区分不同终端的标识符，并且是唯一区分UE外围终端的标志。

注：设备标志的定义请参考3GPP TS33.259。

d）UE接到请求后在本地查找是否具备有效的Ks。如果具备有效的Ks，直接转入步骤h）；如果没有有效的Ks，那么就向BSF发送认证请求。

e）根据GBA过程，收到认证请求的BSF到HSS获取该用户的认证信息。

f）BSF获得认证信息后与UE进行双向认证以及密钥协商，完成用户和BSF之间身份的互相认证及共享密钥Ks的生成。

g）BSF为Ks定义一个有效期并分配一个会话事务标识（B-TID）给用户。

h）UE由Ks计算衍生密钥，计算参数除了Ks，“gba-me”‖RAND‖IMPI‖NAF_ID以外，还包括外围设备的设备标志。即：

如果UICC具备GBA功能，那么则由UICC计算衍生密钥Ks_ext_NAF和Ks_int_NAF：Ks_ext_NAF = KDF（Ks，“gba-me”‖RAND‖IMPI‖NAF_Id‖设备标志）；Ks_int_NAF = KDF（Ks，“gba-u”‖RAND‖IMPI‖NAF_Id‖设备标志）。

如果Ks存放在在ME上（说明UE已经执行了GBA_ME过程），则由ME计算衍生密钥Ks_NAF：Ks_NAF= KDF（Ks，“gba-me”‖RAND‖IMPI‖NAF_Id‖设备标志）。

i）UE通过本地接口将计算出的衍生密钥连同Ks的B-TID一起发送给外围设备的应用客户端（NAF-Client）。

j）外围设备上的应用客户端再次向NAF发送连接请求，并在请求消息中携带B-TID，以及设备标志。

k）NAF先在本地查询是否有用户携带的该B-TID，如果NAF不能在本地查询到该B-TID，则向BSF进行查询，该请求查询消息中携带了NAF标识和B-TID以及设备标志。

l）BSF根据B-TID查找到相应的密钥Ks，并根据B-TID、设备标志以及NAF-ID采用与UE相同算法计算衍生密钥Ks_ext_NAF和Ks_int_NAF（UICC具备GBA能力）或者Ks_NAF（UICC不具备GBA能力）。

另外，BSF还可以根据设备标志来区分某一个用户的不同终端设备，运营商可以直接根据自身策略控制某一用户的访问某一个业务的终端接入数。或者将控制策略发给NAF，例如可以在USS设置相应的标志，运营商进行配置后，由BSF发给NAF，再由NAF进行控制。

m）BSF将衍生密钥连同密钥的有效期一起返回给NAF。

n）接下来NAF便和外围终端设备采用衍生密钥Ks_int_NAF或者Ks_（ext）_NAF通信。

另外，如果NAF对一个用户的多终端连接有一定的限制策略或者从BSF返回的信息中包含运营商的策略，那么NAF可以根据设备标志来区分该用户的不同终端连接，并根据相应策略进行相应处理。例如，如果NAF只允许某用户同一时刻只有一个终端访问NAF或者AS（若某个NAF有多个AS），那么如果发现该用户有新的终端连接请求，可以断开旧的连接，也可以拒绝新的连接请求。

K.1.2 设备标志（Device-ID）方案分析

- 需要更改 Ua 接口和 Zn 接口传递的参数（如 Device ID）
- 需要更改 BSF 和 UE 产生 Ks_NAF 时的参数（如 Device ID）
- 在 GBA_U 的情况下，终端需要把 Device ID 传送给 UICC 卡，用于计算 Ks_NAF
- 可以避免对每个 Device 使用一个 AV，以达到减少 AV 消耗的目的

K.2 终端分离情况下的通用认证解决方案-Hash方案

K.2.1 Hash方案

a）无卡设备上的NAF应用客户端（NAF-Client）向NAF发送请求，如果该客户端知道NAF要求采用GAA密钥进行认证，就跳过这一步骤，直接进入步骤c）。

b）NAF查找该用户是否已经具备有效的密钥。如果没有，指示NAF应用客户端采用GAA密钥与其进行安全通信。

标准分享网 www.bzfxw.com 免费下载

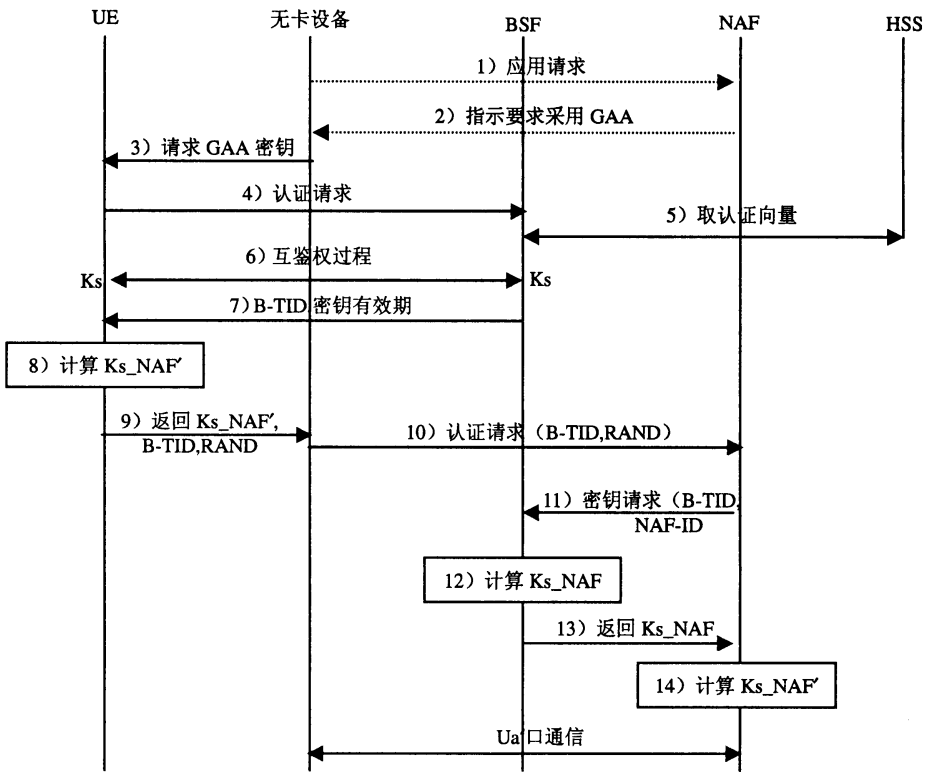


图 K.2　无卡终端的自举过程及建立安全关联过程

c）无卡设备上NAF应用客户端向UE请求NAF衍生密钥，并在请求消息里携带应用标识NAF-ID。

d）UE接到请求后在本地查找是否具备有效的Ks。如果具备有效的Ks，直接转入步骤h）；如果没有有效的Ks，那么就向BSF发送认证请求。

e）根据GBA过程，收到认证请求的BSF到HSS获取该用户的认证信息。

f）BSF获得认证信息后与UE进行双向认证以及密钥协商，完成用户和BSF之间身份的互相认证及共享密钥Ks的生成。

g）BSF为Ks定义一个有效期并分配一个会话事务标识（B-TID）给用户。

h）UE计算出Ks_NAF及Ks_NAF′=HASH（Ks_NAF，RAND）。

i）UE通过本地接口将NAF衍生密钥Ks_NAF′，B-TID和RAND一起发送给无卡设备的NAF应用客户端。

j)无卡设备上的NAF应用客户端再次向NAF发送连接请求，并在请求消息中携带B-TID，以及RAND。

k）NAF先在本地查询是否有用户携带的该B-TID，如果NAF不能在本地查询到该B-TID，则向BSF进行查询，该请求查询消息中携带了NAF标识和B-TID。

l）BSF根据B-TID查找到相应的密钥Ks，并根据B-TID及NAF-ID采用与UE相同算法计算Ks_NAF。

m）BSF将衍生密钥Ks_NAF连同密钥的有效期一起返回给NAF。

n）NAF 计算出 Ks_NAF′=HASH（Ks_NAF，RAND）。

o）NAF便和无卡终端设备采用衍生密钥Ks_NAF′通信。

K.2.2　Hash方案分析

- 需要更改 Ua 接口传输的参数（如 RAND′）
- 该方案中的 RAND 不同于 AV 中的 RAND，需要改为 RAND′，而且需要在终端产生该 RAND′

- 在 Device 丢失 Ks_NAF′或第一次申请 Ks_NAF′时，需要 UE 重新产生一个 RAND′，并由 Ua 接口将该 RAND′传输给 NAF
- 可以避免对每个 Device 使用一个 AV，以达到减少 AV 消耗的目的

K.3 终端分离情况下的通用认证解决方案——正常GBA方案

K.3.1 正常GBA方案

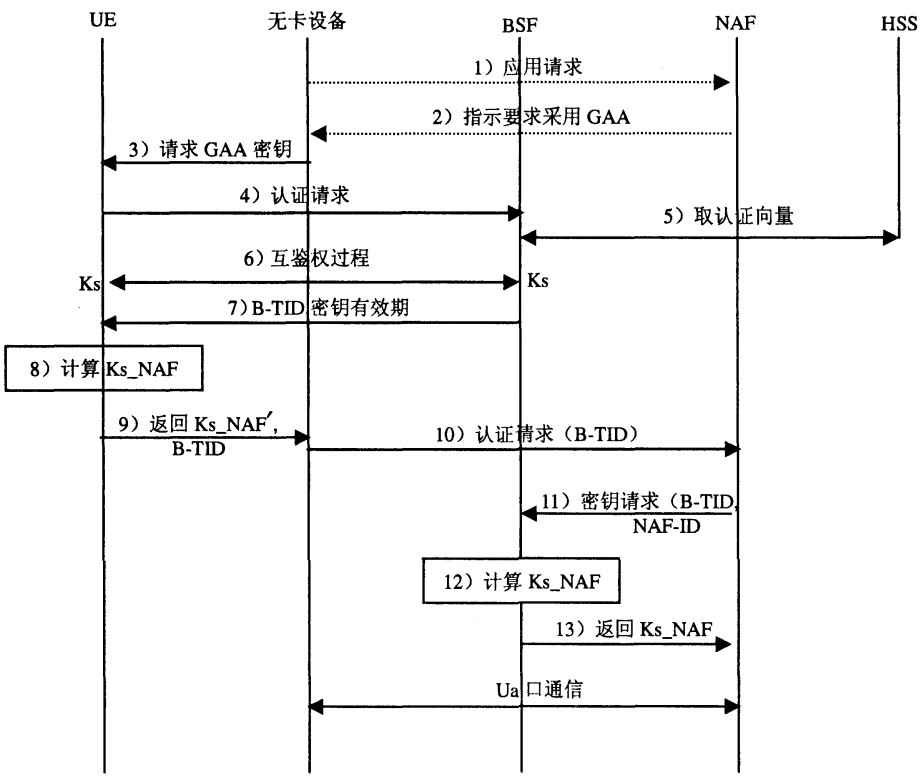


图 K.3 无卡终端的自举过程及建立安全关联过程

a）无卡设备上的NAF应用客户端（NAF-Client）向NAF发送请求，如果该客户端知道NAF要求采用GAA密钥进行认证，就跳过这一步骤，直接进入步骤c）。

b）NAF查找该用户是否已经具备有效的密钥。如果没有，指示NAF应用客户端采用GAA密钥与其进行安全通信。

c）无卡设备上NAF应用客户端向UE请求NAF衍生密钥，并在请求消息里携带应用标识NAF-ID。

d）UE接到请求后就向BSF发送认证请求。

e）根据GBA过程，收到认证请求的BSF到HSS获取该用户的认证信息。

f）BSF获得认证信息后与UE进行双向认证以及密钥协商，完成用户和BSF之间身份的互相认证及共享密钥Ks的生成。

g）BSF为Ks定义一个有效期并分配一个会话事务标识（B-TID）给用户。

h）UE计算出Ks_NAF。

i）UE通过本地接口将NAF衍生密钥Ks_NAF和B-TID 一起发送给无卡设备的NAF应用客户端。

j）无卡设备上的NAF应用客户端再次向NAF发送连接请求，并在请求消息中携带B-TID。

标准分享网 www.bzfxw.com 免费下载

k）NAF先在本地查询是否有用户携带的该B-TID，如果NAF不能在本地查询到该B-TID，则向BSF进行查询，该请求查询消息中携带了NAF标识和B-TID。

l）BSF根据B-TID查找到相应的密钥Ks，并根据B-TID及NAF-ID采用与UE相同算法计算Ks_NAF。

m）BSF将衍生密钥Ks_NAF连同密钥的有效期一起返回给NAF。

n）NAF便和无卡设备采用衍生密钥Ks_NAF通信。

K.3.2 正常GBA方案分析

- 不需要更改原 GBA 接口和协议；
- 对 AV 会有消耗。

参 考 文 献

OMA：“Provisioning内容版本1.1”，版本2003年8月13日. 开放移动联盟。

标准分享网 www.bzfxw.com 免费下载

YD/T 1858-2009

中 华 人 民 共 和 国
通 信 行 业 标 准
2GHz TD-SCDMA/WCDMA 数字蜂窝移动通信网　通用认证架构
（第二阶段）
YD/T 1858-2009
*
人民邮电出版社出版发行
北京市崇文区夕照寺街 14 号 A 座
邮政编码：100061
北京新瑞铭印刷有限公司印刷
版权所有　不得翻印
*
开本：880 × 1230　1/16　　2009 年 8 月第 1 版
印张：6.25　　2009 年 8 月北京第 1 次印刷
字数：169 千字
ISBN 978 - 7 - 115 - 1790/09 - 32
定价：50 元
本书如有印装质量问题，请与本社联系　电话：(010)67114922