(19)中华人民共和国国家知识产权局

(12)发明专利

(10)授权公告号 CN 101156486 B
(45)授权公告日 2011.05.25

(21)申请号 200680010534.6
(22)申请日 2006.01.11
(30)优先权数据
60/652,633 2005.02.14 US
(85)PCT申请进入国家阶段日
2007.09.28
(86)PCT申请的申请数据
PCT/IB2006/000041 2006.01.11
(87)PCT申请的公布数据
WO2006/085170 EN 2006.08.17
(73)专利权人 诺基亚公司
地址 芬兰埃斯波
(72)发明人 P·莱蒂南 P·金斯伯格
(74)专利代理机构 北京市金杜律师事务所 11256
代理人 吴立明
(51)Int.Cl.
H04W 8/12(2009.01)

(56)对比文件
US 2004/0230862 A1,2004.11.18, 全文.
CN 1483164 A,2004.03.17, 全文.
Huawei.S3-040933
Update of GUSS in BSF.《3GPP TSG SA WG3 Security-SA3#36》.2004, 全文.

审查员 靳晶

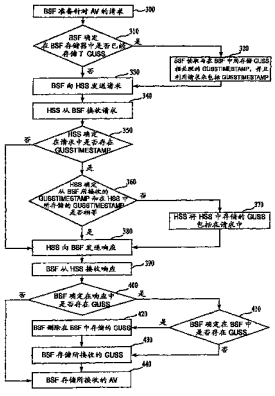
权利要求书 4 页 说明书 94 页 附图 4 页

(54)发明名称

无线通信系统中数据优化传输的方法和装置

(57)摘要

一种用于在通信系统中共享数据的装置和方法,包括配置为发送第一消息的引导服务器功能(BSF)。第一消息包括对应于在BSF中所存储的通用引导架构用户安全设置(GUSS)的时间戳参数。归属用户服务器(HSS),配置用以接收第一消息,用以将对应于在BSF中所存储的GUSS的时间戳参数与对应于在HSS中所存储的GUSS的时间戳参数进行比较,以及在当BSF和HSS的GUSS的时间戳参数相等的时候用以将不包括GUSS的第二消息发送回BSF。



CN 101156486 B

1. 一种用于在通信系统中共享数据的装置，包括：

引导服务器功能 BSF，配置为发送第一消息，其中所述第一消息包括对应于在所述引导服务器功能中所存储的通用引导架构用户安全设置 GUSS 的时间戳参数，并且其中，在归属用户服务器 HSS 处，将对应于在所述引导服务器功能中所存储的所述通用引导架构用户安全设置的所述时间戳参数与对应于在所述归属用户服务器 HSS 中所存储的通用引导架构用户安全设置的时间戳参数进行比较；并且所述引导服务器功能配置为，当所述引导服务器功能和所述归属用户服务器的通用引导架构用户安全设置的所述时间戳参数相等的时候，接收不包括所述通用引导架构用户安全设置的第二消息。

2. 根据权利要求 1 所述的装置，其中所述 BSF 配置为，当所述 BSF 和所述 HSS 的 GUSS 的所述时间戳参数不相等的时候，从所述 HSS 接收包括所述 GUSS 和所述对应时间戳参数的所述第二消息。

3. 根据权利要求 1 所述的装置，其中对应于特定 GUSS 的所述时间戳参数是相同 GUSS 的一部分。

4. 根据权利要求 2 所述的装置，其中所述 BSF 配置用以接收来自所述 HSS 的所述第二消息、所述 GUSS 以及关联于所述 GUSS 的所述时间戳参数，并且配置用以更新来自所述 HSS 的所述 GUSS 和所述时间戳参数。

5. 根据权利要求 1 所述的装置，其中所述第一消息包括针对认证矢量 AV 的请求。

6. 根据权利要求 1 所述的装置，其中所述 HSS 配置为向所述 GUSS 指定所述时间戳参数。

7. 根据权利要求 6 所述的装置，其中所述 HSS 配置为，当所述 GUSS 的数据已经被修改的时候改变用于所述 GUSS 的所述时间戳参数。

8. 根据权利要求 6 所述的装置，其中所述 HSS 配置为以单调增加序列或者单调减小序列来为所述 GUSS 指定所述时间戳参数。

9. 根据权利要求 6 所述的装置，其中所述 HSS 配置为将用于 GUSS 的所述时间戳参数指定为所述 BSF 和所述 HSS 的 GUSS 的特定实例的哈希或者哈希的一部分。

10. 根据权利要求 1 所述的装置，其中所述 BSF 配置为以与所述 HSS 中所存储的所述时间戳参数不同的数字或者字符形式来存储所述时间戳参数。

11. 根据权利要求 1 所述的装置，其中所述 BSF 配置为以与所述 HSS 的所述时间戳参数不同的数字或者字符形式来传输所述时间戳参数。

12. 根据权利要求 6 所述的装置，其中当所述 GUSS 第一次创建的时候，所述时间戳被初始化为数字值、或者初始化为指示由所述 HSS 中的时钟所指示的时间和 / 或日期的值。

13. 根据权利要求 6 所述的装置，其中每次修改所述 GUSS 时，所述 GUSS 变成新版本，并且所述时间戳以 1 递增或者递减，或者所述时间戳变化到由所述 HSS 中的时钟所指示的当前时间和 / 或日期。

14. 根据权利要求 6 所述的装置，其中所述 GUSS 被指定有时间戳值，所述时间戳值是所述 GUSS 的特定实例的哈希或者所述哈希的一部分。

15. 一种用于在通信系统中共享数据的方法，包括：

从引导服务器功能 BSF 向归属用户服务器 HSS 发送第一消息，其中所述第一消息包括对应于在所述引导服务器功能中所存储的通用引导架构用户安全设置 GUSS 的时间戳参

数，并且其中，在所述 HSS 处，将对应于在所述引导服务器功能中所存储的所述通用引导架构用户安全设置的所述时间戳参数与对应于在所述归属用户服务器中所存储的通用引导架构用户安全设置的时间戳参数进行比较；以及

当所述引导服务器功能和所述归属用户服务器的通用引导架构用户安全设置的所述时间戳参数相等的时候，在所述引导服务器功能处接收不包括所述通用引导架构用户安全设置的第二消息。

16. 根据权利要求 15 所述的方法，进一步包括：

当所述 BSF 和所述 HSS 的 GUSS 的所述时间戳参数不相等时，从所述 HSS 向所述 BSF 传送包括所述 GUSS 和所述对应时间戳参数的所述第二消息。

17. 根据权利要求 16 所述的方法，进一步包括：

在所述 BSF 处接收来自所述 HSS 所述第二消息、所述 GUSS 以及关联于所述 GUSS 的所述时间戳参数；以及

在所述 BSF 中更新来自所述 HSS 的所述时间戳参数和所述 GUSS。

18. 根据权利要求 15 所述的方法，其中发送所述第一消息包括发送针对认证矢量 AV 的请求。

19. 根据权利要求 15 所述的方法，其中针对用于所述 GUSS 的所述时间戳的指定以单调增加序列或者单调减小序列来执行。

20. 根据权利要求 15 所述的方法，其中以作为所述 BSF 和所述 HSS 的 GUSS 的特定实例的哈希或者哈希的一部分来执行针对所述 GUSS 的所述时间戳参数的指定。

21. 根据权利要求 15 所述的方法，进一步包括：

以与所述 HSS 中所存储的所述时间戳参数不同的数字或者字符形式来存储所述 BSF 的时间戳参数。

22. 根据权利要求 15 所述的方法，进一步包括：

以不同的数字或字符形式来传送所述 BSF 的所述时间戳参数和所述 HSS 的时间戳参数。

23. 根据权利要求 15 所述的方法，进一步包括：

将所传输的所述时间戳参数的不同数字或者字符形式转换回其初始形式。

24. 根据权利要求 15 所述的方法，进一步包括：

以单调增加序列或者单调减小序列来向所述时间戳指定值。

25. 根据权利要求 15 所述的方法，进一步包括：

当第一次创建所述 GUSS 的时候，将所述时间戳初始化为数字值或由所述 HSS 中的时钟所指示的时间和 / 或日期。

26. 根据权利要求 15 所述的方法，进一步包括：

将所述时间戳以 1 递增或者递减，或者每次修改所述 GUSS 时增加或减小所述时间戳，由此所述时间戳成为新版本。

27. 根据权利要求 15 所述的方法，进一步包括：

每次修改所述 GUSS 时，将所述时间戳改变到所述时间戳的当前时间和 / 或日期。

28. 根据权利要求 15 所述的方法，进一步包括：

指定时间戳值给 GUSS，所述时间戳值是所述 GUSS 的特定实例的哈希或者所述哈希的

一部分。

29. 一种用于在通信系统中共享数据的设备，包括：

用于从引导服务器功能 BSF 向归属用户服务器 HSS 发送第一消息的装置，其中所述第一消息包括对应于在所述引导服务器功能中所存储的通用引导架构用户安全设置 GUSS 的时间戳参数；并且其中，在所述 HSS 处，将对应于在所述引导服务器功能中所存储的所述通用引导架构用户安全设置的所述时间戳参数与对应于在所述归属用户服务器中所存储的通用引导架构用户安全设置的时间戳参数进行比较；以及

用于当所述引导服务器功能和所述归属用户服务器的通用引导架构用户安全设置的所述时间戳参数相等的时候，在所述引导服务器功能处接收不包括所述通用引导架构用户安全设置的第二消息的装置。

30. 根据权利要求 29 所述的设备，进一步包括：

用于当所述 BSF 和所述 HSS 的 GUSS 的所述时间戳参数不相等的时候，从所述 HSS 向所述 BSF 发送包括所述 GUSS 和所述对应时间戳参数的所述消息的装置。

31. 根据权利要求 29 所述的设备，进一步包括：

用于接收来自所述 HSS 的所述消息、所述 GUSS 以及关联于所述 GUSS 的所述时间戳参数的装置；以及

用于在所述 BSF 中更新来自所述 HSS 的所述时间戳参数和所述 GUSS 的装置。

32. 根据权利要求 29 所述的设备，其中发送所述第一消息包括发送针对认证矢量 AV 的请求。

33. 根据权利要求 29 所述的设备，其中以单调增加序列或者单调减小序列来执行针对所述 GUSS 的所述时间戳参数的指定。

34. 根据权利要求 29 所述的设备，其中以作为所述 BSF 和所述 HSS 的 GUSS 的特定实例的哈希或者哈希的一部分来执行针对所述 GUSS 的所述时间戳参数的指定。

35. 根据权利要求 29 所述的设备，进一步包括：

用于以与所述 HSS 中所存储的所述时间戳参数不同的数字或者字符形式来存储所述 BSF 的时间戳参数的装置。

36. 根据权利要求 29 所述的设备，进一步包括：

用于以不同的数字或字符形式来传送所述 BSF 的所述时间戳参数和所述 HSS 的时间戳参数的装置。

37. 根据权利要求 29 所述的设备，进一步包括：

用于以单调增加序列或者单调减小序列来向所述时间戳指定值的装置。

38. 根据权利要求 29 所述的设备，进一步包括：

用于当第一次创建所述 GUSS 的时候，初始化所述时间戳为数字值或由所述 HSS 中的时钟所指示的时间和 / 或日期的装置。

39. 根据权利要求 29 所述的设备，进一步包括：

用于将所述时间戳以 1 递增或者递减，或者每次修改所述 GUSS 时增加或减小所述时间戳的装置，并且所述时间戳成为新版本。

40. 根据权利要求 29 所述的设备，进一步包括：

用于每次修改所述 GUSS 时，将所述时间戳改变到当前时间和 / 或日期的装置。

41. 根据权利要求 29 所述的设备，进一步包括：

用于指定时间戳值给 GUSS 的装置，所述时间戳值是所述 GUSS 的特定实例的哈希或者所述哈希的一部分。

42. 一种通信系统，包括：

网络应用功能 NAF；

用户设备，配置为与所述网络应用功能通信并且用以传送针对认证信息的请求；

引导服务器功能 BSF，配置为接收请求并传送第一消息，其中所述消息包括对应于在所述引导服务器功能中所存储的通用引导架构用户安全设置 GUSS 的时间戳参数；以及

归属用户服务器 HSS，配置为接收所述第一消息，用以将对应于存储在所述引导服务器功能中的所述通用引导架构用户安全设置的所述时间戳参数与对应于存储在所述归属用户服务器中的通用引导架构用户安全设置的时间戳参数进行比较，以及当所述引导服务器功能和所述归属用户服务器的所述通用引导架构用户安全设置的时间戳参数相等的时候，将不包括所述通用引导架构用户安全设置的第二消息传送回所述引导服务器功能。

43. 一种用于在通信系统中共享数据的设备，包括：

传送装置，用于从引导服务器功能向归属用户服务器 HSS 传送第一消息，其中所述第一消息包括对应于在所述引导服务器功能 BSF 中所存储的通用引导架构用户安全设置 GUSS 的时间戳参数，并且其中，在所述 HSS 处，对应于存储在所述引导服务器功能中的所述通用引导架构用户安全设置的所述时间戳参数与对应于存储在所述归属用户服务器中的通用引导架构用户安全设置的时间戳参数进行比较；以及

接收装置，用于当所述引导服务器功能和所述归属用户服务器的通用引导架构用户安全设置的所述时间戳参数相等的时候，在所述引导服务器功能处接收不包括所述通用引导架构用户安全设置的第二消息。

44. 一种用于在通信系统中共享数据的设备，包括：

接收装置，用于接收第一消息，其中所述第一消息包括对应于在引导服务器功能 BSF 中所存储的通用引导架构用户安全设置 GUSS 的时间戳参数；

比较装置，用于将对应于存储在所述引导服务器功能中的所述通用引导架构用户安全设置的所述时间戳参数与对应于存储在所述归属用户服务器中的通用引导架构用户安全设置的时间戳参数进行比较；以及

发射装置，用于当所述引导服务器功能和所述归属用户服务器的通用引导架构用户安全设置的所述时间戳参数相等的时候，将不包括所述通用引导架构用户安全设置的第二消息传送回所述引导服务器功能。

无线通信系统中数据优化传输的方法和装置

[0001] 相关申请的交叉参考

[0002] 本申请要求于 2005 年 2 月 14 日提交的美国临时专利申请序列号 No.60/652,633 的优先权。在此通过参考而引入该较早提交的申请的主题。

技术领域

[0003] 本发明涉及在通信系统中的功能和单元之间用于共享安全数据的装置和方法，且尤其涉及用于确定保护数据有效性以及随后基于该确定结果的数据共享的装置和方法。

背景技术

[0004] 对于世界大部分人口来说，通信系统，且尤其是无线通信系统已经变得日益可用并且负担得起。这些无线通信系统的成功进而导致了适应订户数量大规模增长的需求。处理适应大规模增长需求的一个方法是使得无线通信系统可扩展。另一方法是优化构成无线通信系统的元件和功能。作为结果，通信系统的架构框架已持续演进。

[0005] 一个已经演进的领域是无线通信系统中的认证架构。在无线通信系统中，在进一步通信可发生之前，许多应用在客户端 / 用户设备 (UE) 和应用 / 应用服务器之间共享对相互认证的需求。例子包括但不限于在客户端和在线服务器 (presence server) 之间的通信、或者与内容服务器的通信。因为许多应用共享对对等 (peer) 认证机制的共同需求，所以已经开发了通用认证框架 (GAA)。

[0006] 第三代合作伙伴计划 (3GPP) 通用认证框架 (GAA) 的初始认证 (即，引导 (bootstrap)) 是基于 AKA(认证和密钥协定协议) 的。在由第三代合作伙伴计划 (3GPP) 所制作的文档中描述了 GAA 架构。该文档参考是 3GPP TS 33.919 :“3rd Generation PartnershipProject ;Technical Specification Group Services and System Aspects ; 3G security ;Generic Authentication Architecture(GAA) ;Systemdescription”，该文档作为附录 A 而附加于此，因而其内容通过参考而引入。

[0007] GAA 的一个显著方面在于其包括独立于应用的机制，其向客户端 /UE 和应用 / 应用服务器提供共有的共享秘密。该共享秘密随后可用以认证客户端 /UE 和应用 / 应用服务器之间的无线通信。在由第三代合作伙伴计划 (3GPP) 所制作的文档中描述了这个方面，而该文档参考是 3GPP TS 33.220 :“3rd Generation Partnership Project ; Technical Specification Group Services and System Aspects ;3Gsecurity ;Generic Authentication Architecture(GAA) ;Genericbootstrapping architecture(Release 7)”，该文档作为附录 B 而附加于此，而“3GPP TS 29.109 :3rd Generation Partnership Project ;TechnicalSpecification Group Core Networks and Terminals ; GenericAuthentication Architecture(GAA) ;Zh and Zn Interfaces based on theDiameter protocol ;Stage 3(Release 7)”，该文档作为附录 C 而附加于此，因而其内容通过参考而引入。

发明内容

[0008] 根据本发明的一个实施方式，提供了一种用于在通信系统中共享数据的装置，包括配置为传送第一消息的引导服务器功能 (BSF)，其中第一消息包括对应于在 BSF 中所存储的通用引导架构用户安全设置 (GUSS) 的时间戳参数。归属用户服务器 (HSS) 配置为接收第一消息，用以将对应于存储在 BSF 中的 GUSS 的时间戳参数与对应于存储在 HSS 中的 GUSS 的时间戳参数进行比较，以及用以在当 BSF 和 HSS 的 GUSS 时间戳参数相等的时候，将不包括 GUSS 的第二消息传送回 BSF。

[0009] 根据本发明的一个实施方式，提供了一种用于在通信系统中共享数据的方法，包括将第一消息从引导服务器功能 (BSF) 传送到归属用户服务器 (HSS)，其中第一消息包括对应于在BSF 中所存储的通用引导架构用户安全设置 (GUSS) 的时间戳参数；将对应于存储在 BSF 中的 GUSS 的时间戳参数与对应于存储在 HSS 中的 GUSS 的时间戳参数进行比较；以及在当 BSF 和 HSS 的 GUSS 时间戳参数相等的时候，将不包括 GUSS 的第二消息传送回 BSF。

[0010] 根据本发明的一个实施方式，提供了一种包含在计算机可读介质中的计算机程序，以提供在通信系统中共享数据，包括将第一消息从引导服务器功能 (BSF) 传送到归属用户服务器 (HSS)，其中消息包括对应于在 BSF 中所存储的通用引导架构用户安全设置 (GUSS) 的时间戳参数；将对应于存储在BSF 中的GUSS 的时间戳参数与对应于存储在HSS 中的 GUSS 的时间戳参数进行比较；以及在当 BSF 和 HSS 的 GUSS 时间戳参数相等的时候，将不包括 GUSS 的第二消息传送回 BSF。

[0011] 根据本发明一个实施方式，提供了一种用于通信系统的装置，该通信系统包括：网络应用功能 (NAF)；用户设备，配置为与 NAF 通信并且用以传送针对认证信息的请求；以及引导服务器功能 (BSF)，配置为接收请求并传送第一消息。第一消息包括对应于在BSF 中所存储的通用引导架构用户安全设置 (GUSS) 的时间戳参数。归属用户服务器 (HSS) 配置为接收第一消息，用以将对应于存储在 BSF 中的 GUSS 的时间戳参数与对应于存储在 HSS 中的 GUSS 的时间戳参数进行比较，以及在当 BSF 和 HSS 的 GUSS 的时间戳参数相等的时候，将不包括 GUSS 的第二消息传送回 BSF。

附图说明

[0012] 包括的附图用以对本发明提供进一步的理解并且结合于此构成此说明书的一部分，示意了本发明的实施方式，其与说明书一起用于解释本发明的原理，其中：

[0013] 图 1 示出了根据本发明一个实施方式的提供针对网络应用服务器的通用机制的装置；

[0014] 图 2 是在引导服务器功能和归属用户服务器之间传输信息的例子的一个实施方式；以及

[0015] 图 3A 和图 3B 示出了根据本发明一个实施方式的一种方法，该方法提供了用以最小化流量负载的通用引导架构用户安全设置时间戳。

具体实施方式

[0016] 现在将在下文中参考附图来更全面地描述本发明，其中示出了本发明的某些但并非所有实施方式。实际上，这些发明可以实现为许多不同的形式并且不应理解为构成对在

此阐明的实施方式的限制；相反，提供这些实施方式以便本公开满足适用的法律要求。贯穿全文，相同的标号表示相同的元件。

[0017] 3GPP GBA 是提议（3GPP TS 33.220 作为附录 B 附加于此，而 3GPP TS 29.209 作为附录 C 附加于此，因而其内容通过参考引入）的认证架构。可以使用此架构以使得在网络侧的和在用户侧的应用功能能够在网络侧和用户侧不能另外进行通信的情况下来通信。此功能称为“应用安全性的引导”，或者更通常地简化为“引导”。

[0018] 引导的一般原则是，通用引导服务器功能 (BSF) 允许用户设备 (UE) 与之认证，并就会话密钥达成协定。这种认证可以基于认证和密钥协定 (AKA)。通过运行 AKA，移动终端和网络彼此相互认证并且就密钥达成协定，特别是机密性密钥 (CK) 和完整性密钥 (IK)。在此认证之后，UE 和网络应用功能 (NAF)（其还可称为服务提供商）可以运行一些应用专用协议，其中消息的认证是基于在 UE 和 BSF 之间达成协定的会话密钥。

[0019] 引导功能并不旨在于依赖任何特定网络应用功能。实现引导功能的服务器必须受到归属运营商的信任以处理认证向量。在运营商的归属网络、受访网络、或者第三方网络中可以支持网络应用功能。

[0020] 图 1 示出了根据本发明一个实施方式的示范性网络架构。网络架构包括用户设备 (UE) 100、至少一个网络应用功能 (NAF) 102、引导服务器功能 (BSF) 104、以及归属用户系统 (HSS) 106。BSF 104 和 HSS 106 形成归属移动网络运营商 (MNO) 108 的一部分。UE 100 根据公知的移动通信技术而连接到 MNO 108。

[0021] 例如，NAF 102 在 MNO 108 控制之下被主控于网元中，而 BSF104 也在 MNO 108 控制之下被主控于网元中。由此，为了实践目的，NAF 102 和 BSF 104 的每个可以认为是网元。另外，MNO 108 可以包括控制器（未示出）以执行将在图 3A 和图 3B 中描述的操作。控制器可以包括永久的或者可移除的存储器，诸如磁盘和光盘、RAM、ROM 等，在其上可以存储和分布本发明的处理和数据结构。

[0022] 如在图 1 中所示，UE 100 通过 Ua 接口 110 与 NAF 102 通信。UE 100 通过 Ub 接口 112 与 BSF 104 通信。NAF 102 通过 Zn 接口 114 与 BSF 104 通信。BSF 104 通过 Zh 接口 116 与 HSS 106 通信。

[0023] 在进一步分离的网络中可以提供 NAF 102。例如，如图 1 中所示，提供了一个示范性网络架构，其中 NAF 102 位于受访网络之中。在当 UE 100 接触 NAF 102（其在归属网络以外的其它网络中操作）的情况下，此受访 NAF 102 可以使用 NAF 网络的直径代理 (D-Proxy) 来与订户的 BSF（即，归属 BSF）104 通信。然后 NAF 102 将通过至 D-Proxy 的 Zn 接口 114 并且通过至 BSF 104 的 Zn 接口 120 来与 BSF 104 通信。

[0024] 对于图 1，引导的原理在于，UE 100 和引导服务器功能彼此互相认证，例如使用 AKA 协议，并且就主共享秘密达成协定。之后，使用主共享的秘密来得出一个或者多个网络应用功能专用共享的秘密，该秘密应用在 UE 100 和所讨论的特定 NAF 之间。特别地，针对每个网络应用功能而独立地生成 NAF 专用共享秘密密钥资料。在已经完成引导操作之后，UE 100 和网络应用功能可以运行某些专用协议，其中消息的安全将基于在 UE 100 和引导服务器功能之间的相互认证期间所生成的那些密钥。由此，密钥可以用于认证和完整性保护并用于机密性。然后，网络应用功能能够获取 NAF 专用共享秘密，该专用共享秘密从在用户设备和引导服务器功能之间建立的主共享秘密中得出。

[0025] 此外，通信 Ub 接口 112 支持引导认证和密钥协定协议，以在 UE 100 和 BSF 104 之间提供相互认证和密钥协定。Zh 接口 116 允许 BSF 104 从 HSS 106 取得任何所需的认证信息和订户配置信息（例如，认证矢量，AV）。订户的用户安全性设置 (USS) 集是订户的 GUSS 的一部分，其可以存储在 HSS 中。在一个人具有多个订制的情况下，即在通用移动通信系统集成电路卡 (UICC) 上有多个 IP 多媒体子系统订户识别模块卡 (ISIM) 或者通用订户识别模块卡 (USIM) 应用的情况下，HSS 106 将包含可映射到任何一个或者多个标识上的一个或者多个 GUSS，该标识例如是 IP 多媒体私有标识 (IMPI) 和国际移动订户标识 -IMSI。Ua 接口 110 支持任何应用专用协议，其使用 NAF 专用共享秘密（根据由 Ub 接口 112 所支持的协议，从 UE 100 和 BSF 104 之间达成协定的主共享秘密所获取）来保护。NAF 102 使用 Zn 接口 114 从 BSF 104 获取从主共享的秘密中所得到的 NAF 专用共享秘密，其中该主共享秘密在 Ub 接口 112 上支持的协议中达成协定。Zn 接口 114 还可以用以从 BSF 104 获取订户配置信息。

[0026] 从 BSF 104 传送到 NAF 102 的消息包括引导信息。引导信息可以包括事务标识符、NAF 专用共享秘密、以及订户配置信息（“prof_naf”或者“任何 NAF 特定 USS”）。

[0027] 此外，通用引导架构用户安全设置 (GUSS) 集还可以包括在引导信息和所有应用专用 USS 集中。通常，BSF 请求用于特定订户的 AV，然后还接收随被请求 AV 一起的订户的 GUSS。在操作期间，BSF 104 能够在一时间通过 Zh（来自 BSF 104 的 HSS 接口）从 HSS106 取回单一认证矢量 (AV)，因而当 UE 100 由 BSF 104 引导的时候，使 BSF 104 通过来自 HSS 106 的 GUSS 的新副本来更新存储在其中的 GUSS。因此，如果 NAF 102 需要从 BSF 104 获取一个或多个更新的 USS，则 NAF 102 需要请求 UE 100 以通过 BSF 104 进行引导，即重新协商，而在 NAF 102 下一次从 BSF 104 请求特定 GUSS 的时候，NAF 102 知道 GUSS 是更新过的。

[0028] 然而，此更新过程使 HSS 106 在每次请求新 AV 的时候发送 GUSS，而无论从 BSF 104 最后一次接收到 GUSS 以来在 HSS 106 中 GUSS 是否已经更新。在更新过程期间，通过发送带有 GUSS 的 AV，由于 GUSS 的尺寸可以很大，这使得在 BSF 104 和 HSS 106 之间的流量负载很大。即使在 BSF 104 已经具有相同 GUSS 副本的情况下，也向 BSF 104 发送 GUSS 是不必的，而这将导致带宽和计算机资源的浪费。因而，需要将从 HSS 106 向 BSF 104 传送 GUSS 的次数最小化。

[0029] 为此，本发明的装置和方法配置并传送 GUSS，以包括从 HSS 106 到 BSF 104 的时间戳，以将关于在 BSF 104 和 HSS 106 之间的 GUSS 传输过程的流量负载最小化。因而，本发明的装置和方法通过确定各种安全数据的有效性并且随后根据确定结果来共享数据而允许在通信系统中的功能和元件之间共享受保护的数据，。

[0030] 根据本发明的实施方式，仅当请求或者接收网元对在传输或者源网元上存在的完全相同的数据不具有副本或不能访问的时候，传输网元或者源网元（例如 GBA 中的 HSS 106）中的数据被传送至或由请求网络或者接收网元（例如 GBA 中的 BSF 104）共享。

[0031] 因而，GUSS 时间戳添加到每个 GUSS，指示 GUSS 何时最后一次由 HSS 106 所改变。此时间戳用以优化 HSS 106 和 BSF 104 之间的 GUSS 传送策略。如果 BSF 104 在其需要获取用于订户的新认证矢量 (AV) 的时候在存储器中具有订户的 GUSS，则它还将 GUSS 时间戳包括在请求中。一旦接收到 GUSS 时间戳，HSS 106 将该时间戳与其数据库中所存储的 GUSS 时间戳进行比较。如果时间戳相等，则由于 BSF 104 已经具有 GUSS 的副本，因而 HSS 106 不

将GUSS发送到BSF 104。如果时间戳不相等，则因为BSF 104具有需要被更新的无效GUSS，因而HSS 106发送GUSS。如果HSS 106不具有GUSS，例如因为已经使用HSS的管理接口删除了GUSS，则HSS 106将不发送GUSS消息到BSF 104，而BSF 104将删除旧的GUSS。

[0032] 图2示出了根据本发明一个实施方式的、在包括GUSS时间戳的HSS 106和BSF 104之间的通信。在操作150处，UE 100发布针对新引导的请求，该引导包括涉及UE 100的用户身份信息。当BSF104正在取回或者请求来自HSS 106的新AV的时候，在操作152处，如果GUSS已经存在、或者已经存储在BSF 104的存储器中（即，BSF存储器），则针对新AV的请求还将包括GUSS时间戳。一旦接收到GUSS时间戳，则HSS 106检查并且将该GUSS时间戳与在其中提供的存储器（即，HSS存储器）中所存储的GUSS时间戳进行比较。在操作154处，如果从BSF 104所接收到的GUSS时间戳和在HSS 106中所存储的GUSS时间戳不同，则HSS 106将更新的GUSS，针对该更新的GUSS的GUSS时间戳以及所请求的新AV包括在一起。如果GUSS时间戳相同，即，BSF 104存储器中的GUSS和HSS 106中的GUSS相同，则并不将GUSS随同所请求的新AV发送到BSF 104。

[0033] 自然，仅当BSF 104在BSF存储器中具有针对特定订户的GUSS的时候，GUSS时间戳可以从BSF 104发送到HSS 106。在此例中，GUSS时间戳不发送到HSS 106，而HSS 106将订户专用GUSS从其中的数据库返回到BSF 104。

[0034] 在操作156处，BSF 104在消息中将随机质询数据(RAND)和认证标志(AUTN)转发到UE 100，用以请求UE 100自身对其认证。在操作158处，关联于UE 100的客户端运行认证和密钥协定(AKA)算法、校验AUTN、并且获得认证结果(RES)。UE 100还计算机密性密钥(CK)、完整性密钥(IK)和RES，这将在BSF 104和UE 100两者中得到相同的会话密钥IK和CK。在操作160处，UE 100将包含使用RES计算出来的AKA响应的超文本传输协议(HTTP)请求发送到BSF 104。在操作162处，BSF 104通过校验AKA响应来认证UE 100。在操作164处，BSF 104通过串接(concatenate)CK和IK来生成密钥资料(Ks)。在操作166处，BSF 104将OK消息和引导事务标识符(B-TID)以及密钥Ks的寿命发送到UE 100以指示认证成功。另外，在操作168处，UE 100以与BSF 104在操作164中相同的生成方式来生成密钥资料(Ks)，并且存储Ks.B-TID以及Ks的寿命。

[0035] 因而，HSS 106中的每个GUSS包括新的时间戳参数，例如标记的GUSSTIMESTAMP(GUSS时间戳)。GUSS的GUSSTIMESTAMP由HSS 106来设置，而GUSSTIMESTAMP是指示当HSS 106修改GUSS时的最后时间的数字或者字符参数。GUSSTIMESTAMP参数还可以指示GUSS数据的版本。GUSSTIMESTAMP在GUSS内容变化的时候变化。即，如果在HSS 106中的GUSS被修改或者更新，则HSS 106为更新的GUSS分配新的GUSSTIMESTAMP。

[0036] GUSSTIMESTAMP还可以以与存储GUSSTIMESTAMP的方式等效或者不同的形式（例如，数字或者字符）来存储或传送，或者连同GUSS存储在HSS 106中。然而，如果以不同形式存储或者传送，则GUSSTIMESTAMP的这种改变的形式可以转换回到HSS 106中GUSSTIMESTAMP的原始表示。例如，当需要比较多个GUSSTIMESTAMP的时候，执行这种转换。

[0037] 根据本发明的一个方面，BSF 104从HSS 106接收GUSS或者其等同物，并且在BSF存储器中存储GUSS。当BSF 104从HSS 106中请求AV的时候，而其先前已经接收到对应的GUSS时，则请求可以包括GUSSTIMESTAMP。HSS 106将所接收的GUSSTIMESTAMP与已经

存储在 HSS 106 中的 GUSSTIMESTAMP 进行比较，并且只有在两个 GUSSTIMESTAMP 不同的时候在回复中包括 GUSS。两个 GUSSTIMESTAMP 可能不同，例如，当 BSF 104 具有无效或者过时的 GUSS 时。如果 GUSSTIMESTAMP 相等，则 HSS 106 将不会将 GUSS 随 AV 发送到 BSF 104。

[0038] 图 3A 示出了根据本发明实施方式的用以创建和修改 GUSSTIMESTAMP 的方法。GUSSTIMESTAMP 的初始化发生在当创建特定的 GUSS 的时候。在操作 200 处，HSS 106 创建 GUSS。在操作 210 处，HSS 106 初始化 GUSSTIMESTAMP。无论何时特定的 GUSS 被修改，都将执行 GUSSTIMESTAMP 的更新操作。在操作 220 处，HSS 106 修改 GUSS。在操作 230 处，HSS 106 更新 GUSSTIMESTAMP。

[0039] 可存在多个方法，用以在针对 HSS 中特定 GUSS 指定 GUSSTIMESTAMP 参数的值。在本发明的一个实施方式中，可以由单调增加序列或者单调减小序列来指定 GUSSTIMESTAMP。例如，当第一次创建 GUSS 的时候，可以将 GUSSTIMESTAMP 指定或初始为某数字值，或者指定或初始为由 HSS 106 中的时钟所指示的时间和 / 或日期。每次修改 GUSS，则因而成为一个新的版本，例如 GUSSTIMESTAMP 可以 1 递增或者递减或者变化到由 HSS 106 中的时钟所指示的当前时间和 / 或日期。在另一实施方式中，GUSS 可以指定为这样的 GUSSTIMESTAMP 值，该值是 GUSS 的特定实例的哈希或者哈希的一部分，诸如 SHA-1 或者 MD5。

[0040] 图 3B 示出了根据本发明实施方式的一种方法，该方法提供了用以最小化流量负载的通用引导架构用户安全设置时间戳。在操作 300 处，该方法在 BSF 104 处准备针对认证矢量 -AV 的请求。在操作 310 处，在 BSF 104 处确定 GUSS 是否已经存储在 BSF 存储器中。如果该方法确定已经存储了 GUSS，则在操作 320 处，方法在 BSF 104 处读取关联于在 BSF 104 中所存储的 GUSS 的 GUSSTIMESTAMP，并且利用请求来包括 GUSSTIMESTAMP。然而，如果方法确定在 BSF104 中未存储 GUSS，则在操作 330 处，方法在 BSF 104 处向 HSS 106 发送请求。

[0041] 在操作 340 处，方法在 HSS 106 处接收来自 BSF 104 的请求。在操作 350 处，由 HSS 106 确定在请求中是否存在 GUSSTIMESTAMP。如果方法确定在请求中存在 GUSSTIMESTAMP，则在操作 360 处，方法在 HSS 106 处确定从 BSF104 所接收的 GUSSTIMESTAMP 和在 HSS 106 中所存储的 GUSSTIMESTAMP 是否相等。否则，如果方法确定在请求中不存在 GUSSTIMESTAMP，则在操作 350 之后，方法前进到操作 380，这将在下文中描述。

[0042] 在操作 360 处，如果方法确定从 BSF 104 所接收的 GUSSTIMESTAMP 和在 HSS 106 中存储的 GUSSTIMESTAMP 相等，则方法前进到操作 380，否则方法前进到操作 370。在操作 370 处，方法将存储在 HSS 106 中的 GUSS 包括在响应中并且前进到操作 380。

[0043] 在操作 380 处，该方法将 HSS 106 配置为向 BSF 104 发送响应。在操作 390 处，BSF 104 从 HSS 106 接收响应。在操作 400 处，方法在 BSF 104 处确定在响应中是否存在 GUSS。如果在响应中存在 GUSS，则在操作 410 处，方法在 BSF 104 处确定在 BSF 104 中是否已经存在 GUSS。否则，方法前进到操作 440，这将在下文中描述。如果方法确定在 BSF 104 中存在 GUSS，则方法前进到操作 420。否则，方法前进到操作 430，这将在下文中描述。

[0044] 在操作 420 处，该方法在 BSF 104 处删除在 BSF 104 中所存储的 GUSS，并且前进到操作 430。在操作 430 处，该方法在 BSF 104 处存储所接收的 GUSS，而在操作 440 处，BSF 104 存储所接收的 AV。

[0045] 应理解，在本发明的实施方式中以示出的序列和方式执行操作，尽管某些操作等

可以有所变化而并不背离本发明的精神和范围。

[0046] 因而，本发明提供了向在 BSF 和 HSS 之间交换的每个 GUSS 增加 GUSS 时间戳，该时间戳指示了 HSS 何时最后改变 GUSS。GUSS 时间戳将 BSF 和 HSS 之间的数据传输策略优化。具体而言，当通过用户设备从订户请求用以获取新认证矢量的请求的时候，如果 BSF 具有关联于在存储器中所存储的订户的数据，则新 AV 请求还包括与在 BSF 的存储器中存储的 GUSS 相关联的 GUSS 时间戳。一旦接收到 GUSS 时间戳，则 HSS 将 GUSS 时间戳与在 HSS 存储器中存储的 GUSS 时间戳进行比较。如果 GUSS 时间戳相同或者相等，则由于 BSF 已经具有 GUSS 的副本因而 HSS 不向 BSF 发送 GUSS。如果 GUSS 时间戳不相等，则由于 BSF 具有需要更新的无效 GUSS，因而 HSS 发送 GUSS。

[0047] 另外，尽管在本发明的说明中已经使用了分组和数据报这样的术语，但本发明对许多类型的网络数据都很重要。为了本发明的目的，术语分组包括分组、单元、帧、数据报、桥接协议数据单元分组、分组数据及其任意等同物。

[0048] 从详细说明书中，本发明的许多特征和优点都变得清楚明了，且由此所附权利要求书旨在于覆盖落入本发明的精神和范围之内的本发明的所有这样的特征和优点。此外，由于对于本领域技术人员容易做出许多修改和变化，因而并不期望将本发明的范围限制到所示出和描述的精确架构和操作，因而可以采取的所有适当的修改和等同物都落入本发明的范围之中。

[0049] 附录 A

[0050] 3GPP TR 33.919 V6.2.0(2005-03)

[0051] 技术报告

[0052] 第三代伙伴计划；

[0053] 技术规范组服务和系统方面；

[0054] 3G 安全；

[0055] 通用认证架构 (GAA)；

[0056] 系统描述

[0057] (版本 6)

[0058] 本文档已经在第三代伙伴计划 (3GPP™) 中开发并且可以针对 3GPP 的意图进一步详细阐述。

[0059] 本文档还没有经过 3GPP 组织伙伴的任何同意处理过程并且尚未被实现。

[0060] 提供此规范仅在 3GPP 内部用于进一步的开发工作。组织伙伴不接受对于使用此规范的任何义务。

[0061] 对于 3GPP™ 系统实现的规范和报告应该通过 3GPP 组织伙伴的出版办公室获得。

[0062] 关键字

[0063] UMTS，认证，安全，GAA

[0064] 3GPP

[0065] 通信地址

[0066] 3GPP 支持办公室地址

[0067] 650 Route des Lucioles-Sophia Antipolis

[0068] Valbonne-FRANCE Tel. :+33492944200 Fax :+33493654716

[0069] 因特网

[0070] http://www.3gpp.org

[0071] 版权声明

[0072] 除了通过书面许可的授权之外没有部分可以复制。

[0073] 版权和前述限制扩展到所有媒体中的复制。

[0074] © 2005,3GPP Organizational Partners(ARIB,ATIS,CCSA,ETSI,TTA,TTC)。

[0075] All Right reserved

[0076] 3GPP

[0077] 目录

[0078] 前言.....4

[0079] 介绍.....4

[0080] 1范围.....5

[0081] 2参考.....5

[0082] 3定义和缩略语.....6

[0083] 3.1定义.....6

[0084] 3.2缩略语.....6

[0085] 4通用认证架构.....7

[0086] 4.1 GAA概述.....7

[0087] 4.2使用共享秘密认证.....7

[0088] 4.3基于（公有,私有）密钥对和证书的认证.....7

[0089] 5发布认证凭证.....8

[0090] 5.1示意性概述.....8

[0091] 5.2 GBA:发放共享秘密的机制.....8

[0092] 5.3 SSC:发放用户证书的机制.....8

[0093] 6 GAA结构模块.....9
[0094] 6.1 GAA结构总览.....9
[0095] 6.2 GAA.....9
[0096] 6.3 GBA.....9
[0097] 6.4 SSC.....10
[0098] 6.5使用HTTPS访问网络应用功能.....10
[0099] 6.5.1有鉴权代理的HTTPS.....10
[0100] 6.5.2无鉴权代理的HTTPS.....10
[0101] 7使用GAA的应用指南.....11
[0102] 7.1共享秘密和GBA的使用.....12
[0103] 7.2证书的使用.....12
[0104] 附录A：更改历史.....13

[0105] 前言

[0106] 此技术报告已经由第三代伙伴计划（3GPP）制作。

[0107] 本文档的内容服从TSG中的连续工作并且可以随着正式的TSG同意改变。一旦TSG修改本文档的内容，TSG将通过带有发布日期和如下增加的版本号的可识别变化来对其进行重新发布：

[0108] 版本x.y.z

[0109] x第一个数字

[0110] 1呈现给TSG用于信息

[0111] 2呈现给TSG用于同意

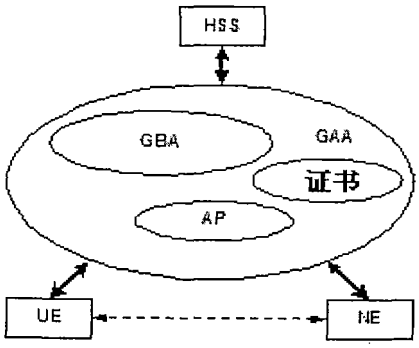
[0112] 3或者更大指示修改控制下的TSG同意文档

[0113] y第二个数字增大用于所有实质的修改，即技术增强、修正、更新等。

[0114] z当仅编辑性修改已经合并于该文档中时第三个数字增大。介绍

[0115] 此节提供关于GAA上下文的介绍以及一些为何撰写此TR的解释（带有一些对于三个相关技术规范的参考）。

[0116]



[0117] 图 1 :GAA 的示意图

[0118] 很多应用都需要在进一步的通信前，在客户端（即 UE）和应用服务器之间进行双向认证。例子包括（但不限于）客户端和在线服务器（可能通过认证代理）间的通信，客户端申请数字证书时与 PKI 端口的通信，与内容服务器、BM-SC 等等的通信。

[0119] 由于许多应用都需要同级别的认证机制，定义一种通用认证架构 (GAA) 已经被认为是有用的。此 GAA 描述了一种用于可以优先服务任何（现在和将来）的应用的同级通用认证架构。

[0120] 此 TR 可以被考虑作为如图 1 中说明的通用认证架构的框架文档。GBA、AP 和证书是 GAA 的构造模块并且它们被指定在每个分离的 TS 中。它们在 GAA 中怎样组合在本文档中解释。

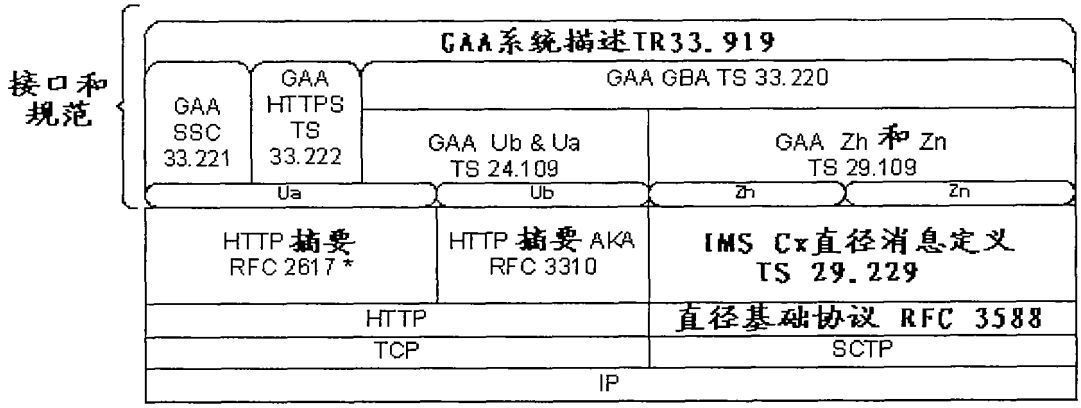
[0121] 1 范围

[0122] 此 3 GPP 技术报告目的是给出移动应用可以依靠的用于在服务器和客户端（即 UE）之间进行认证的不同机制的概述。另外，它提供了关于 GAA 的使用以及在给定情况中并且用于给定应用的认证机制的选择的引导。

[0123] 为此，TR 将关于同级认证的不同 GAA 规范放到前瞻中。澄清了用于具有三个技术规范的逻辑，拟定了它们的内容并且解释这三个 TS 和它们与此 TR 的关系间的相互联系。

[0124] 图 1 描述了 GAA 接口上使用的协议和不同 GAA 规范间的关系。当它们有效时，新的 GAA 规范将被添加到该图。将来也可以添加其它协议。特别是，将来可以添加 Ua 接口的新种类并且然后在 Ua 接口下面可以添加其他协议。

[0125]



[0126] GAA 在 Ua 接口上能潜在支持许多协议。一个例子是 HTTP 摘要。

[0127] 图 2 :GAA 规范与 GAA 接口使用的协议之间的关系

[0128] 2 参考

[0129] 下列文档包含通过此文本中的参考的规定，组成本文档的规定。

[0130] ●参考是特定的（由出版日期、印刷号、版本号等识别）或非特定的。

[0131] ●对于特定参考，后续修改不适用。

[0132] ●对于非特定参考，应用最新版本。在参考 3GPP 文档（包括 GSM 文档）的情况中，非特定参考隐含地指与当前文档具有相同版本的文档的最新版本。

[0133] 3GPP TS 33.102：″ 3rd Generation Partnership Project ;Technical Specification Group Servicesand System Aspects ;3G Security ;Sccurity architecture″ .

[0134] 3GPP TS 33.220：″ 3rd Generation Partnership Project ;Technical Specification Group Servicesand System Aspects ;3G Security , Generic Authentication Architecture (GAA) ;Genericbootstrapping architecture″ .

[0135] 3GPP TS 33.221：″ 3rd Generation Partnership Project ;Technical Speclfication Group Servicesand System Aspects ;3G Security ;Generic Authentication Architecture (GAA) ;Support forsubscriber certificates″ .

[0136] 3GPP TS 33.222 ″ 3rd Generation Partnership Project ;Technical Specification Group Servicesand System Aspects ;3G Security Gencric Authentication Archltecture (GAA) ;Access to networkapplication tunctions using secure hypcrtext transfer protocol (HTTPS)″ .

[0137] IETF RFC 2818：″ HTTP Over TLS″ .

[0138] 3GPP TS 29.109：″ 3rd Gencratlon Partnership Project ;Technical Specification Group CoreNetwork ;Gencric Authentication Architecture (GAA) ;Zh and Zn Interfaces based on the Diameter protocol ;Protocol details″ .

[0139] 3GPP TS 24.109：″ 3rd Generation Partnership Project ;Technical Specification Group CoreNetwork ;Bootstrapping Interface (UB) and Network application function interface (Ua) ;Protocoldetails″ .

[0140] 3GPP TS 29.198-03：″ 3rd Generation Partnership Project ;Technical Specification Group CoreNetwork ;Open Service Access (OSA) ;Application Programming Interface (API) ;Part 3 ;Framework″ .

[0141] 3GPP TS 29.199-01：″ 3rd Generation Partnership Project ;Technical Specification Group CoreNetwork ;Open Servlce Access (OSA) ;Parlay X web services ;Part 1 ;Common″ .

[0142] 3 定义和缩略语

[0143] 3.1 定义

[0144] 出于本文档的目的，应用下列术语和定义。

[0145] 用户证书：基于他 / 她的订阅，由移动网络运营商向用户发放的证书。它包含用户拥有的公有密钥和可能的其他信息，例如某些形式的用户身份。

[0146] 3.2 缩略语

[0147] 出于本文档的目的，应用下列缩略语。

[0148] AKA 认证和密钥协定

[0149] AP 认证代理

[0150] AS 应用服务器

[0151] BSF 引导服务器功能

[0152] GAA 通用认证架构

[0153] GBA 通过引导架构

[0154] HSS 归属用户系统

[0155] NAF 网络应用功能

[0156] NE 网元

[0157] PKI 公有密钥基础结构

[0158] SSC 对于用户证书的支持

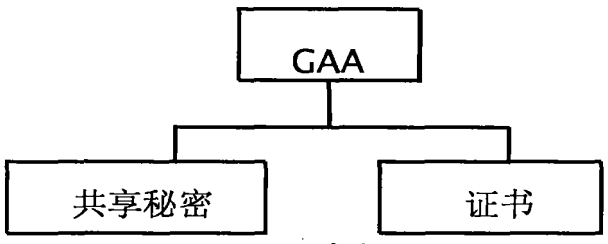
[0159] UE 用户设备

[0160] 4 通用认证架构

[0161] 4.1 GAA 概述

[0162] 一般来说存在两种认证机制。一种基于通信实体间的共享秘密，另一种基于（公有，私有）密钥对和数字证书。如图 3 所示，在 GAA 中这个两个对于移动应用而言可优先应用的选项。

[0163]



[0164] 图 3 :GAA 示意概述

[0165] 4.2 使用共享秘密的认证

[0166] 存在基于通信实体间预共享秘密的若干个认证协议。常有的例子包括 HTTP 摘要，具有预共享秘密 IKE 和基于用户名和密码的任何现有机制。

[0167] 这些机制的主要问题在于如何在该预共享秘密上达成一致。5.2 节和 GBA TS 33.220[2] 描述了如何在移动的上下文环境中使用基于 AKA 的机制为两个通信实体提供预共享秘密。

[0168] 4.3 基于（公有，私有）密钥对和证书的认证

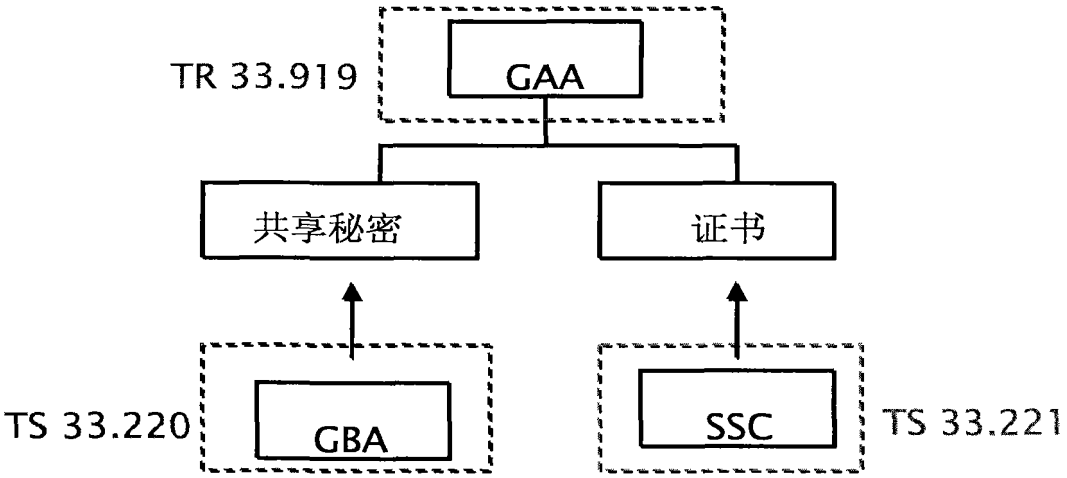
[0169] 对于使用共享秘密认证外可选的是依靠非对称密码。这假设需要认证的实体（通信单方或者双方）拥有（公有，私有）密钥对以及相应的数字证书。后者验证该密钥对并将该密钥对绑定到其合法拥有者。众所周知的基于（公有，私有）密钥对认证的协议包括 PGP 和 TLS 上的 HTTP，RFC 2818[5]（后者常用其协议标识符“HTTPS”称呼）。

[0170] 这类认证的主要缺点在于需要 PKI 并且非对称的密钥密码操作经常基本上比对称的密钥操作需要更多的计算开销。5.3 节和 SSC TS33.221[3] 描述了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）。

[0171] 5 发布认证凭证

[0172] 5.1 示意性概述

[0173]



[0174] 注 :用于发放认证凭证的其他机制可以存在,但都超出本 TR 的范围。

[0175] 图 4 :发放认证凭证机制的示意图

[0176] 图 3 说明了本 TR 与 TS 33.220[2] 以及 TS 33.22 1[3] 之间的关系。一方面,存在基于共享秘密和 GBA 的认证方法,描述于 TS 33.220[2] 中,指定了一种向通信方提供这样的共享秘密的机制。另一方面,存在依靠 (公有,私有) 密钥对和数字证书以及 SSC 的认证方法,描述于 TS33.221[3] 中,指定了如何向移动用户发放证书。

[0177] 5.2 GBA :发放共享秘密的机制

[0178] TS 33.220[2] 指定了基于 3GPP AKA 机制的一种独立于应用的机制,以向客户端和应用服务器提供公共的共享秘密。随后,该共享秘密可以用于认证客户和应用服务器之间的通信。

[0179] 5.3 SSC :发放用户证书的机制

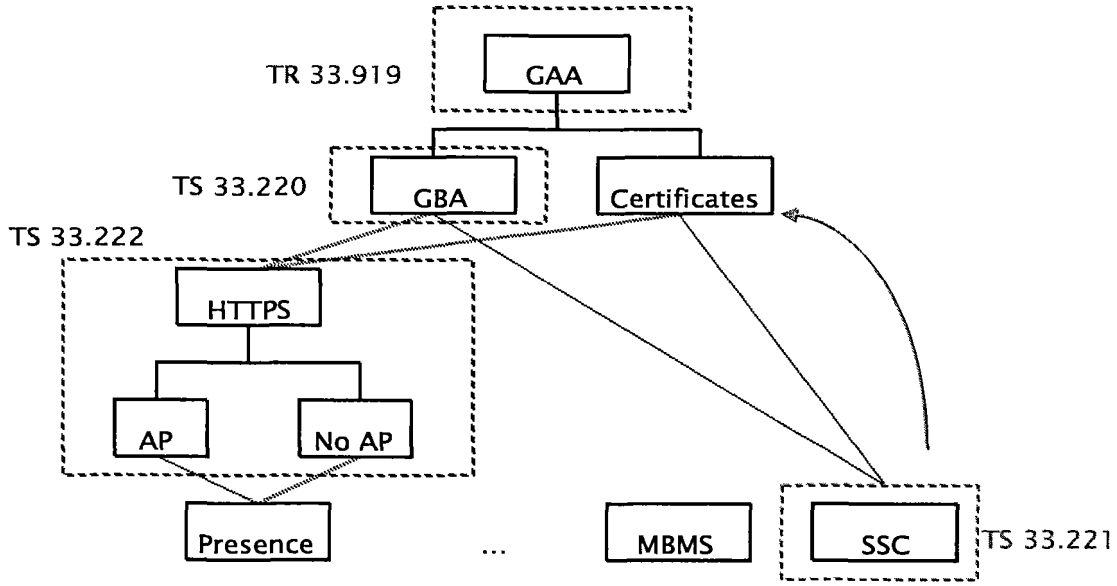
[0180] TS 33.221[3],指定了向移动用户发放数字证书的机制。

[0181] 一旦移动用户拥有 (公有,私有) 密钥对并且已为其获得证书,则他可以一起使用该证书和相应的密钥以在例如移动电子商务应用中创建数字签名而且也可以向服务器认证 (如 TLS 中)。

[0182] 6 GAA 结构模块

[0183] 6.1 GAA 结构概述

[0184]



[0185] 图 5 :GAA 结构模块的相互关系详细总览

[0186] 本节给出了不同 GAA 文档的内容的高级概述，并描述了这些文档如何适应在一起。

[0187] 6.2 GAA

[0188] GAA 是指描述了通用认证框架的通用框架的此 TR。

[0189] 6.3 GBA

[0190] 如 5.2 节指示的概要，GBA 基于 3GPP AKA 提供通用机制以在 UE 和服务器间安装共享秘密。

[0191] AKA 是移动网络所用的一种非常强大的机制。GBA 得到本机制的益处并且重用 AKA 以引导应用安全。GBA 引入了一个称作引导服务器功能 (BSF) 的新网元 (NE)。该 BSF 具有与 HSS 的接口。UE 通过 BSF 使用 HSS 运行 AKA。根据该结果 (CK、IK)，在 BSF 和 UE 中产生一个会话密钥。应用服务器（在 TS 33.220[2] 中称为网络应用功能 (NAF)）可以从 BSF 获得该会话密钥和用户档案信息。以这种方式，应用服务器 (NAF) 和 UE 共享密钥，该共享密钥可以随后用于应用安全，特别是在应用会话的开始时用于认证 UE 和 NAF（也可能用于完整性保护和 / 或机密性保护，尽管完整性保护和机密性保护可能在 GAA 的范围中不严格）。UE 和 BSF 之间和 NAF 和 BSF 之间以及 BSF 和 HSS 之间的通信是独立于应用，并在 TS 33.220[2] 中描述。

[0192] 以下观点导致了新 NE(BSF) 的引入 :

[0193] 将从 HSS 检索 AV 的所有不同类型的 NE 的数量以及 NE 的总数量保持最小。

[0194] 一个用于不同应用的通用机制避免了机制间的大的差异性并且允许以一致的方式一次阐述安全问题。

[0195] 6.4 SSC

[0196] 如果一个客户想使用非对称加密技术，他需要一个由认证机构 (CA) 创建的数字证书。这样的数字证书将公开密钥绑定到其合法拥有者的身份上，并且证明该公开密钥的合法性。如果移动用户想拥有并且使用（公有，私有）密钥对，该密钥对和证书应该被预先加载或该用户必须具有生成或获取密钥对并且动态地获得相应的数字证书的方法。如 5.3

节中所是概要描述，SSC 指定机制以动态地向移动用户发布数字证书。

[0197] 为动态地获得数字证书，UE 必须发送适当的证书请求到他归属运营商的 PKI 入口，并且该 PKI 入口必须认证该证书请求。证书注册过程即发放证书给用户和在 UE 和 PKI 入口之间的相应通信会话事实上是移动应用实例。就如很多移动应用，它需要通信实体的认证，在此情况下是 UE 和 PKI 入口（后者扮演应用服务器的角色）。对于任何其他应用，对于此认证存在两个选项：基于预共享秘密或者基于非对称密码以及证书。后者是当从 PKI 入口请求新证书时而另一个仍旧有效的证书已经加载在 UE 中时仅有的选项。前一方法在 PKI 入口和 UE 之间需要共享秘密。如果该共享秘密不是提前配置的，则 GBA 可以被使用以获得这样共享秘密。

[0198] 如图 4 所示，描述于 SSC TS33.221[2] 中的向移动用户发放证书的处理过程的结果是 UE 加载相应有对应于其（公有，私有）密钥对的证书。这由绿色向上的箭头所示。

[0199] 一旦该证书就绪，它可以用于（和相应的（公有，私有）密钥对一起）认证该 UE。这由连接证书到下面应用（图 4 中的 HTTS 和 SSC）的黑色虚线所示。（公有，私有）密钥对和相应的数字证书也可以用于完整性保护（或极少用于机密性），但这些都不是 GAA 范围的一部分。

[0200] 6.5 使用 HTTPS 访问网络应用功能

[0201] 可以想象，HTTPS（或 HTTP/TLS）可以用在大量服务中以保护 UE 和应用服务器之间的应用会话（TS 33.222 中的 Ua 接口，见 TS33.222[4]）。TS 33.222[4] 描述了当 HTTPS 用于 UE 和应用服务器之间时的可能的认证选项的细节。任何已有或将来的基于 HTTPS 的应用就认证的细节以及安全 HTTPS 会话的建立可以参考 TS 33.222[4]。

[0202] 6.5.1 有认证代理的 HTTPS

[0203] TS 33.222[4] 描述了其中在 UE 和 AS 之间使用反向代理（称为认证代理 (AP)）的一种机制。

[0204] AP 是 TLS 的端点并且 UE 应能同时连接到位于一个 AP 之后的不同 AS。AP 应能使用 GAA 的方式认证 UE，并且应该发送认证过的 UE 身份给 AS。如果 UE 认证是基于共享秘密的，那么 AP 在 GAA 架构和术语中担任 NAF。

[0205] 使用这样的 AP 的可能优势可以包括减少认证矢量的消耗，最小化 SQN 同步失败以及减少 UE 需要建立和保持的 TLS 会话的数目。

[0206] 6.5.2 无认证代理的 HTTPS

[0207] 基于 HTTP 的应用服务也可以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。在该情况下，AS 应该能够使用 GAA 的方式认证 UE。如果 UE 的认证是基于共享秘密的，那么 AS 在 GAA 架构和术语中担任 NAF。

[0208] 7 使用 GAA 的应用指南

[0209] GAA 向 AS 或 AP 提供了不同选择以执行用户认证（即如 TS

[0210] 33.220[2] 中所描述的强迫 UE 使用 BSF 运行 AKA 或使用基于用户证书的机制）。还在 GAA 下，AS 可以明白该用户请求已经由认证代理认证。

[0211] 在 TR 中描述的 GAA 不具有将任何一种认证机制强加到应用上的意图。而它的目的是作为开发者部署的工具，他们可以按照其利益来使用。通过使用 GAA 代替设计和实现应用专用的认证机制，应用开发者可以节省开发时间。GAA 机制的额外优势是它们可以提供

从 GSM/UMTS 继承覆盖继承而来的全球覆盖。

[0212] 依靠运营商的网络配置和策略，AS 或 AP 将能够使用由 GAA 提供的任何选项，或者甚至 3GPP 之外指定的其他用户认证机制，如果这样的机制处于它们的部属。因此，假设 AS 和 AP 应该能够决定使用 GAA 的哪些部分（如果存在的话）。

[0213] 本章试图给出可以在认证机制的选择中扮演角色的观点的概述。认证机制的选择依赖于：

[0214] 1. 相关于需要认证的用户 / 服务器 / 应用 / 设备的需要 / 策略。这也许是处于两个方向上（相互认证），但通常强调的是用户到服务器的认证。

[0215] 2. 用户配置里所定义的设备和服务的特征，用户能力和优选项。

[0216] 3. 提供传输服务的网络以及应用的服务提供商的策略。

[0217] 与认证相关的需求 / 策略将依赖于是否存在下列需要：

[0218] a) 设备认证：设备真实有效而非克隆，即 (U)SIM 认证质询响应 .

[0219] b) 完整性保护：例子是 UTRAN 接入中的信令保护。GSM 的弱点是对于中间人非常容易操纵信令消息例如密码模式命令以及阻止它被威胁的方式是使用设备认证，并通过对特定信令消息上的加密 MAC（消息认证码）达到的完整性保护。

[0220] c) 应用认证：将经常需要验证应用软件的确实性。例子是 TS 29.198-03[8] 和 TS 29.199-01[9]。然而应用认证在 GAA 的范围之外。

[0221] d) 用户认证：这这是指终端用户、正在使用终端用户设备的人的认证。做到此认证的一个方式是逻辑上通过用户 PIN 输入，或物理上通过移除或插入策略来使得 USIM 可用性依赖于设备 / 协议 / 应用。也可以在访问前要求 PIN 的输入，其对于特定应用是允许的。

[0222] e) 事务认证和反抵赖性：对于一些使用移动设备进行的商业事务，有必要使用用户的私有密钥对该交易进行数字签名，尤其是其中存在对于反抵赖性的需要以阻止下列情况时：

[0223] - 消息发送 (SENDING) 的欺诈否认，如“我从未发送过它”

[0224] - 消息的内容 (CONTENT)，如“我说过你应出售，而不是买”

[0225] - 消息的时间 (TIME)，如“我在不同时间发送了它”

[0226] 注意：诸如 3GPP AKA 的许多认证技术都是基于在网络和用户间共享的单一密钥。这对于发送者和接收者之间的认证是可行的 (OK)，但可以向第三方证明的反抵赖可以要求使用公有密钥技术，其中私有密钥仅由发送者拥有。

[0227] 图 5 示出了设备和业务特征如何影响从认证机制的范围中进行特定技术的选择。

[0228]

	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	客户端私有密钥,签名	签名	私有密钥,签名
GAA :GBA	共享秘密	共享秘密	X

[0229]

at UE	(GBA),锁定的 MAC	(GBA),锁定的 MAC 码或服务器私有密钥,签名	

[0230] X :客户特征不满足认证要求。

[0231] 图 5 :认证特征比较

[0232] 7.1 共享秘密和 GBA 的使用

[0233] 其中来自于 GBA 的革新的共享密钥的一些实例可以被使用的是 :

[0234] - 对称加密和完整性密钥的分发,这些密钥能保护运行在网络中的 UE 和服务器之间的应用的安全。可以用于保护应用安全并且需要共享密秘的例子协议包括 HTTP 摘要、共享秘密 TLS 和 IPsec ;

[0235] - 用于第三方应用的口令和 PIN 的分发 ;

[0236] - 用于保护 UE 和认证机构 (CA) 之间证书的分发。

[0237] 7.2 证书的使用

[0238] 其中证书可以用于认证的一些实例是 :

[0239] - 当必须验证终端用户的身份时 ;

[0240] - 当应用安全协议与 (公有,私有) 密钥对认证合作顺利并且用户证书是有效的 (例如,正常 TLS) 时 ;

[0241] - 其中存在对于反抵赖性的需要,并且由于诸如 3GPP AKA 的很多认证技术是基于单一密钥的,所以用户被要求使用用户的私有密钥对交易进行数字签名,该单一密钥在网络和用户间共享。可向第三方证明的反抵赖性可以要求使用公有密钥技术,其中私有密钥仅由发送者拥有。

[0242] 附录 A :更改历史

[0243]

更改历史								
日期	TSG #	TSG Doc.	CR	Rev	主题 / 意见	旧	新
2003-10	SA3#30				新草案 TR :通用认证架构 (GAA)		0.1.0
2003-	SA3#				文本已经被添加到介绍和章 1 到 6	0.1.0	0.2.0

[0244]

11	31						

2003-12	SP-22	SP-030582	-	-	对于 TSG SA#22 的用于信息的呈现	0.2.0	1.0.0
2004-01	SA3#32	-	-	-	编辑性更改加额外的参考	1.0.0	1.0.1
2004-02	SA3#32	-	-	-	已经添加参考。6.5 节中的编者提示已经被移除。已经添加带有解释的图添加并且已经将文本添加到6.3、6.4、6.5 和 7 节。	1.0.1	1.2.0
2004-06	SP-24	SP-040365	-	-	对于 TSG SA#24 用于信息的呈现的编辑性更改	1.2.0	1.2.1
2004-07	SA3#34	-	-	-	已经将文本添加到第 7 章	1.2.1	1.3.0
2004-09	SP-25	SP-040625	-	-	由 MCC 编辑的对 TSG SA#25 用于同意的呈现	1.3.0	2.0.0
2004-09	-	-	-	-	在 TSG SA 同意之后更新到 v6.0.0	2.0.0	6.0.0
2004-12	SP-26	SP-040861	002	-	移除不必要的编者提示	6.0.0	6.1.0
2005-03	SP-27	SP-050140	003	-	更正“使用 GAA 的应用指南”	6.1.0	6.2.0

[0245] 附录 B

[0246] 3GPP TS 33.220 V7.1.1(2005-10)

[0247] 技术报告

[0248] 第三代伙伴计划；

[0249] 技术规范组服务和系统方面；

[0250] 通用认证架构 (GAA)；

[0251] 通用引导架构

[0252] (版本 7)

[0253] 本文档已经在第三代伙伴计划 (3GPP™) 中开发并且可以针对 3GPP 的意图进一步详细阐述。

[0254] 本文档还没有经过 3GPP 组织伙伴的任何同意处理过程并且尚未被实现。

[0255] 提供此规范仅在 3GPP 内部用于进一步的开发工作。组织伙伴不接受对于使用此规范的任何义务。

[0256] 对于 3GPP™ 系统实现的规范和报告应该通过 3GPP 组织伙伴的出版办公室获得。

[0257] 关键字

[0258] UMTS,访问,安全,IP,多媒体,SIP

[0259] 3GPP

[0260] 通信地址

[0261] 3GPP 支持办公室地址

[0262] 650 Route des Lucioles-Sophia Antipolis

[0263] Valbonne-FRANCE

[0264] TeI. :+33492944200 Fax :+33493654716

[0265] 因特网

[0266] http://www.3gpp.org

[0267] 版权声明

[0268] 除了通过书面许可的授权之外没有部分可以复制。

[0269] 版权和前述限制扩展到所有媒体中的复制。

[0270] © 2005,3GPP Organizational Partners(ARlB,ATIS,CCSA,ETSI,TTA,TTC)。

[0271] All Right reserved

[0272] 3GPP

[0273] 目录

[0274] 前言 6

[0275] 1 范围 8

[0276] 2 参考 8

[0277] 3 定义、缩略语符号和约定 10

[0278] 3.1 定义 10

[0279] 3.2 缩略语符号 11

[0280] 3.3 符号 11

[0281] 3.4 约定 11

[0282] 4 通用引导架构 12

[0283] 4.1 参考模型 12

[0284] 4.2 网元 13

[0285] 4.2.1 引导服务器功能 (BSF) 13

[0286] 4.2.2 网络应用功能 (NAF) 14

[0287] 4.2.2a 直径协议 (D 代理) 14

[0288] 4.2.3 HSS 14

[0289] 4.2.4 UE 15

[0290] 4.2.5 SLF 15

[0291] 4.3 引导架构和参考点 16

[0292] 4.3.1 参考点 Ub 16

[0293] 4.3.2 参考点 Ua 16

[0294] 4.3.3 参考点 Zh 16

[0295] 4.3.4 参考点 Zn 16

[0296] 4.3.5 参考点 Dz 16

[0297] 4.4 引导的要求和原理 16

[0298] 4.4.1 接入独立性 17
[0299] 4.4.2 认证方法 17
[0300] 4.4.3 漫游 17
[0301] 4.4.4 参考点 Ub 的要求 17
[0302] 4.4.5 参考点 Zh 的要求 17
[0303] 4.4.6 参考点 Zn 的要求 18
[0304] 4.4.7 引导事物标示符的要求 19
[0305] 4.4.8 UICC 应用的选择和相关密钥的要求 19
[0306] 4.4.9 参考点 Ua 的要求 20
[0307] 4.4.10 参考点 Dz 的要求 21
[0308] 4.5 过程 21
[0309] 4.5.1 引导的初始化 21
[0310] 4.5.2 引导过程 21
[0311] 4.5.3 使用引导安全关联的过程 23
[0312] 4.5.4 涉及服务发现的过程 26
[0313] 5 基于 UICC 增强的通用引导架 (GBAJU) 26
[0314] 5.1 用于带有基于 UICC 增强的引导的架构和参考点 26
[0315] 5.2 带有基于 UICC 增强的引导的要求和原理 26
[0316] 5.2.1 UE 的要求 26
[0317] 5.2.2 BSF 的要求 27
[0318] 5.3 用于带有基于 UICC 增强的引导的过程 27
[0319] 5.3.1 引导的初始化 27
[0320] 5.3.2 引导过程 27
[0321] 5.3.3 使用引导安全关联的过程 29
[0322] 5.3.4 涉及服务发现的过程 32
[0323] 附录 A :空 33
[0324] 附录 B(标准化的) :密钥衍生函数 KDF 的规范 34
[0325] B.1 介绍 34
[0326] B.2 通用密钥衍生函数 34
[0327] B.2.1 输入参数编码 34
[0328] B.3 GBA 和 GBA_U 中 NAF 专用密钥衍生 35
[0329] 附录 C :空 36
[0330] 附录 D(资料性的) :GBA 中使用的 UICC 应用的用户选择的对话框实例 ... 37
[0331] 附录 E(标准化的) :用于保证 Zn 的参考点安全的 TLS 简档 38
[0332] 附录 F(资料性的) :TLS 证书的处理 39
[0333] F.1 TLS 证书注册 39
[0334] F.2 TLS 证书撤销 39
[0335] 附录 G(标准化的) :GBA_U UICC-ME 接口 40
[0336] G.1 GBA_U 引导过程 40

[0337] G.2 GBA_U NAF 衍生过程 40
[0338] 附录 H(标准化的) :Ua 安全协议标示符 42
[0339] H.I 定义 42
[0340] H.2 组织八位字
[0341] 节 42
[0342] H.3 用于 3GPP 指定协议的 Ua 安全协议标示符 42
[0343] 附录 I(标准化的) :2G GBA..... 44
[0344] 1.1 参考模型 44
[0345] 1.2 网元 44
[0346] 1.2.1 引导服务器功能 (BSF)..... 44
[0347] 1.2.2 网络应用功能 (NAF)..... 44
[0348] I.2.2a 直径协议 (D 代理)..... 45
[0349] 1.2.3 HSS..... 45
[0350] 1.2.4 UE..... 46
[0351] 1.3 引导架构和参考点 46
[0352] 1.3.1 参考点 Ub..... 46
[0353] 1.3.2 参考点 Ua..... 46
[0354] 1.3.3 参考点 Zh..... 46
[0355] 1.3.4 参考点 Zn..... 46
[0356] 1.4 引导的要求和原理 46
[0357] 1.4.1 接入独立性 47
[0358] 1.4.2 认证方法 47
[0359] 1.4.3 漫游 47
[0360] 1.4.4 参考点 Ub 的要求 47
[0361] 1.4.5 参考点 Zh 的要求 47
[0362] 1.4.6 参考点 Zn 的要求 48
[0363] 1.4.7 引导事物标示符的要求 49
[0364] 1.4.8 UICC 应用的选择和 SIM 卡的求 49
[0365] 1.4.9 参考点 Ua 的要求 50
[0366] 1.5 过程 50
[0367] 1.5.1 引导的初始化 50
[0368] 1.5.2 引导过程 50
[0369] 1.5.3 使用引导安全关联的过程 53
[0370] 1.5.4 涉及服务发现的过程 55
[0371] 1.6 TLS 简档 55
[0372] 1.6.1 保护机制 56
[0373] 1.6.2 BSF 的认证 56
[0374] 1.6.3 UE 的认证 56
[0375] 1.6.4 安全参数的建立 56

[0376] 附录 J(资料性的):BSF 中带有本地策略加强的 USS 的使用 57
[0377] J.1 综述 57
[0378] J.2 使用场景 57
[0379] J.2.1 场景 1:NAF 不使用 USS,BSF 不具有用于 NAF 的本地策略 58
[0380] J.2.2 场景 2:NAF 不使用 USS,BSF 具有用于 NAF 的本地策略 58
[0381] J.2.3 场景 3:NAF 使用 USS,BSF 不具有用于 NAF 的本地策略 58
[0382] 32.4 场景 4:NAF 使用 USS,BSF 具有用于 NAF 的本地策略 59
[0383] 附录 K(资料性的):更改历史 60

[0384] 前言

[0385] 此技术报告已经由第三代伙伴计划 (3GPP) 制作。

[0386] 本文档的内容服从TSG中的连续工作并且可以随着正式的TSG同意改变。一旦TSG修改本文档的内容,TSG将通过带有发布日期和如下增加的版本号的可识别变化来对其进行重新发布:

[0387] 版本 x.y.z

[0388] x 第一个数字

[0389] 1 呈现给 TSG 用于信息

[0390] 2 呈现给 TSG 用于同意

[0391] 3 或者更大指示修改控制下的 TSG 同意文档

[0392] y 第二个数字增大用于所有实质的修改,即技术增强、修正、更新等。

[0393] z 当仅编辑性修改已经合并于该文档中时第三个数字增大。1 范围

[0394] 本文档描述了安全特征和引导认证的机制以及来自于 3GPP AKA 机制的用于应用安全的密钥协定。使用此引导机制的候选应用包括但不限于用户证书分发 TS33.221[5]。用户证书支持其提供得到移动运营商辅助得服务,以及移动运营商提供的服务。

[0395] 此规范的范围包括通用 AKA 引导功能、架构概述和如何引导凭证的详细过程。

[0396] 此规范的第 4 章描述了称作 GBA_ME 的机制,以引导认证以及密钥协议,其不需要对 UICC 进行任何改变。此规范的第 5 章描述了称作 GBA_U 的机制以引导认证以及密钥协议,其尽管需要对UICC进行改变,但是通过在UICC上存储特定衍生密钥来提供增强的安全性。2 参考

[0397] 下列文档包含通过此文本中的参考的规定,这些规定组成本文档的规定。

[0398] ●参考是特定的(由出版日期、印刷号、版本号等识别)或非特定的。

[0399] ●对于特定参考,后续修改不适用。

[0400] ●对于非特定参考,应用最新版本。在参考 3GPP 文档(包括 GSM 文档)的情况中,非特定参考隐含地指与当前文档具有相同版本的文档的最新版本。

[0401] 3GPP TS 31.102: "3rd Gencration Partnership Project;Technical Specification Group Terminals;Characteristics of the USIM application".

[0402] 3GPP TS 33.102: "3rd Generation Partnership Project;Technical Specification Group Servicesand System Aspeets;3G Security;Security architecture".

[0403] Franks J., et al,: "HTTP Authentication;Basic and Digest Access

Authentication″，RFC 2617，June1999.

[0404] A.Niemi，et al，：″ Hypertext Transfer Protocol(HTTP)Digest Authentication Using Authenticationand Key Agreement(AKA)″，RFC 3310，September 2002.

[0405] 3GPP TS33.221：″ 3rd Generation Partnership Project；Technical Specification Group Serviccsand System Aspects；Genertic Authentication Architecture(GAA)；Support for SubscriberCertificates″.

[0406] T.Dierks，et al，：″ The TLS Protocol Vcrsion 1.0″，RFC 2246.January 1999.

[0407] OMA：″ Provisioning Content Veraion 1.1 ″，Version 13-Aug-2003. Open-Mobile Alliance.

[0408] 3GPP TS 23.228：″ 3rd Generation Partnership Project；Technical Specification Group Servicesand System Aspects；IP Multimcdia Subsystem(IMS)；Stage2(Release 6)″.

[0409] IETF RFC 3546(2003)：″ Transport Layer Security(TLS)Extensions″.

[0410] 3GPP TS31.103：″ 3rd Generation Partncrship Project；Technical Spccification Group Terminals；Characteristics of the IP Multirnedia Scrvices Ldentity Module(ISIM)application″.

[0411] 3GPP TS 23.003：″ 3rd Generation Partncrship Project；Technical Specification Group CoreNetwork；Numbering，addressing and identification″.

[0412] IETF RFC 3548(2003)：″ The Base16，Besc32，and Basc64 Data Encodings″.

[0413] 3GPP TS 33.210：″ 3rd Generation Partnership Project；Technical Specification Group Servlcesand System Aspects；3G Securlty；Network domain secnrity；IP network layer security″.

[0414] IETF RFC 3588(2003)：″ Diarncter Base Protocol″.

[0415] 3GPP TS 31.101：″ 3rd Generation Partnership Project；Technical Specifieation Grop Terminals；UICC-terminal interface；Physical and logical characteristics″.

[0416] 3GPP TS 33.203：″ 3rd Generation Partnership Project；Technical Specification Group Servicesand System Aspects；3G securlty；Access security for IP-based services″.

[0417] IETF RFC 3280(2002)：″ Internet X.509 Public Key Infrastructure Certificale and CertificateRevocation Llst(CRL)Profile″.

[0418] IETF RFC 2818(2000)：″ HTTP over TLS″.

[0419] 3GPP TS 33.310：″ 3rd Generation Partnership Project；Technical Specification Group Service andSystem Aspects；Network Domain Security(NDS)；Authentication Framework(AF)″.

[0420] IETF RFC 2560(1999)：″ X.509 Internet Public Key Infrastructure Online Certificate StatusProtocol-OCSP″.

[0421] FIPS PUB 180-2(2002)：″ Secure Hash Standard″ .

[0422] IETF RFC 2104(1997)： ″ HMAC :Keyed-Hashing for Message Authentication″ .

[0423] ISO/EC 10118-3 :2004； ″ Information Technology-Security technlques-Hash-functions-part3 :Dedlcated hash-functions″ .

[0424] IETF RFC 3629(2003)：″ UTF-8,a transformation format of ISO 10646″ .

[0425] 3GPP TS 33.222： ″ 3rd Generation Partcership Project ;Technical Specification Group Servicesand System Aspects ;Generic Authcntication Architecture(GAA) ;Access to network applicationfunctions using Hypertext Transfer Protocol over Tranport Layer Security(HTTPS)″ .

[0426] 3GPP TS 33.246： ″ 3G Security ;Security of Multimedia Broadcast/Multicast Service(MBMS)″ .

[0427] IETF Internet-Droft″ Pre-Shared Key Ciphersuites for Transport Layer Security(TLS) ″ .Decernber 2005，URL :http://www.jelf.org/intemet-drafts/draft-letf-tls-psk-09.txt.

[0428] IETF RFC 2246(1999)：″ The TLS Protocol Version 1″ .

[0429] 3GPP TS 24.109 :3rd Generation Partnership Project ;Technical Specification Group CoreNetwork and Terminals ;Bootstrapping interface(Ub)and network application function interface(Ua) ;Protocol decails″ .

[0430] OMA WAP-219-TLS,4.11.2001 :http://www.openrnobitealliance.org/tech/affliates/wap/wap-219-tls-20010411-a.pdf.

[0431] OMA WAP-211-WAPCert,22.5.2001 :http:/www.openmobilteatliance.org/tech/affjliates/wap/wap-211-wapcert-20010522-a.pdf.

[0432] 3 定义、缩略语符号和约定

[0433] 3.1 定义

[0434] 出于本文档的目的，应用下列术语和定义。

[0435] 应用 :此文档中的所有地方，其中使用术语应用指由 MNO 或者第三方向移动用户提供的服务，那么，它总是表示应用的类型而不是安装在应用服务器上的应用的实例。

[0436] 引导服务器功能 :BSF 在 MNO、BSF、HSS 的控制下驻留在网元中，并且 UE 参与 GBA，在该 GBA 中通过运行引导过程在网络和 UE 间建立共享密钥。该共享密钥可以在 NAF 和 UE 间使用，例如，用于认证目的。

[0437] 引导使用过程 :在 Ua 参考点上使用引导安全关联的过程。

[0438] GBA 功能 :在使用 BSF（即，支持 Ub 参考点）执行引导过程并且将安全关联提供给 Ua 应用以运行引导使用过程的 ME 上的功能。当 Ua 应用想使用引导的安全关联时，GBA 功能由 Ua 应用调用。

[0439] 基于 ME 的 GBA :在 GBA_ME 中，所有 GBA 专用功能在 ME 中执行。UICC 是不察觉 GBA 的。如果术语 GBA 用于本文档中而没有任何进一步的条件，那么总是代表 GBA ME，见本规范第 4 章。

[0440] 基于 UICC 的 GBA :这是具有基于 UICC 增强的 GBA。在 GBA_U 中，GBA 专用功能在

ME 和 UICC 之间被分开，见本规范第 5 章。

[0441] 网络应用功能 :NAF 驻留于网元中。GBA 可以在 NAF 和 UE 间为了认证的目，以及为了保证 UE 和 NAF 之间的通信路径安全而使用。

[0442] 引导事务标识符 :引导事务标识符 (B-TID) 被用于将用户身份绑定到参考点 Ua、Ub 和 Zn 中的加密资料上。

[0443] GBA 用户安全设置 :GUSS 包含 BSF 特定信息元素和所有应用专用的 USS 的集合。

[0444] GUSS 时间戳 :GUSS 的时间戳由 HSS 建立。无论 HSS 何时修改 GUSS，其都发生改变。

[0445] NAF 组 :NAF 分组以允许将不同 USS 分配到代表相同应用的 NAF。此分组在每个归属网络中分开完成，即，一个联系在不同归属网络中的 BSF 的 NAF 属于每一个归属网络中的不同组。

[0446] NAF_Id :NAF 的全 DNS 名称与 Ua 安全协议标识符连接。

[0447] Ua 应用 :意图使用 NAF 来运行引导使用过程的 ME 上的应用。

[0448] Ua 安全协议标识符 :与 Ua 上的安全协议相关联的标识符。

[0449] 用户安全设置 :USS 是应用和用户指定参数集合，其定义了两部分，认证部分包含应用需要的用户身份列表（例如，IMPU、MSISDN、假名），和授权部分包含用户许可标记（例如对允许应用的访问，可以发布的证书类型）。另外，USS 可以包含密钥选择指示，其用于 GBA_U 情况中以托管 (mandate) 基于 ME 的密钥 (KS_(ext)_NAF) 或者基于 UICC 的密钥 (KS_int_NAF) 或者以上两者的使用。有时也称作应用专用的用户安全设置。USS 从 HSS 传递到 BFS 作为 GUSS 的一部分，并且如果 NAF 请求则从 BSF 传递到 NAF。

[0450] 3.2 缩略语

[0451] 出于本文档的目的，应用下列缩略语 :

[0452] AK :匿名密钥

[0453] AKA :认证和密钥协议

[0454] B-TID :引导事务标识符

[0455] BSF :引导服务器功能

[0456] CA :证书机构

[0457] FQDN :全资格域名

[0458] GAA :通用认证架构

[0459] GBA :通用引导架构

[0460] GBA_ME :基于 ME 的 GBA

[0461] GBAJJ :具有基于 U1CC 增强的 GBA

[0462] GUSS :GBA 用户安全设置

[0463] HSS :归属用户系统

[0464] IK :完整性密钥

[0465] KDF :密钥衍生函数

[0466] Ks_int_NAF :UICC 上保留的 GBA-U 中的衍生密钥

[0467] Ks_ext_NAF :GBAJJ 中衍生密钥

[0468] MNO :移动网络运营商

[0469] NAF :网络应用功能

[0470] PKI :公有密钥基础结构

[0471] SLF :用户定位功能

[0472] USS :用户安全设置

[0473] 3.3 符号

[0474] 出于本文档的目的,应用下列缩略语 :

[0475] ‖ :连接

[0476] ⊕ :异或

[0477] 3.4 约定

[0478] 此规范中的所有数据变量使用左手侧的最高位子串和右手侧最低位子串表示。子串可能是比特、八位字节或者其他任意长度的比特串。当变量被分解成大量子串时,最左(最高)子串编号为 0,次高位编号为 1,依次类推直到最低位。

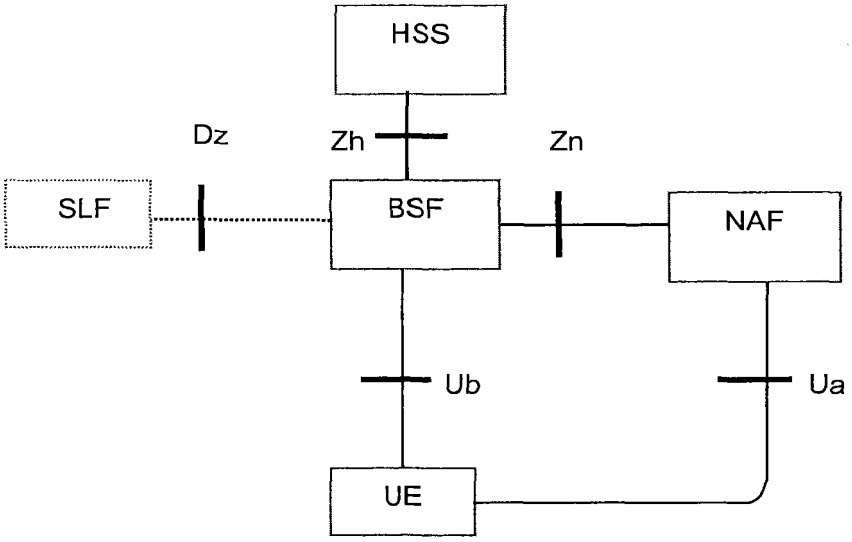
[0479] 4 通用引导架构

[0480] 3GPP 认证基础设施包括了 3GPP 认证中心 (AuC)、USIM 或 ISIM,以及运行在它们之间的 3GPP AKA 协议,并且是 3GPP 运营商非常有价值的资产。已经认识到此基础设施有助于支持网络中的应用功能并且在用户侧建立共享密钥。因此,3GPP 可以通过定义基于 AKA 协议的通用引导架构 (GBA) 来提供“应用安全的引导”以认证用户。

[0481] 4.1 参考模型

[0482] 图 4.1 示出了包含在引导方法中实体的简单网络模型和它们之间使用的参考点。

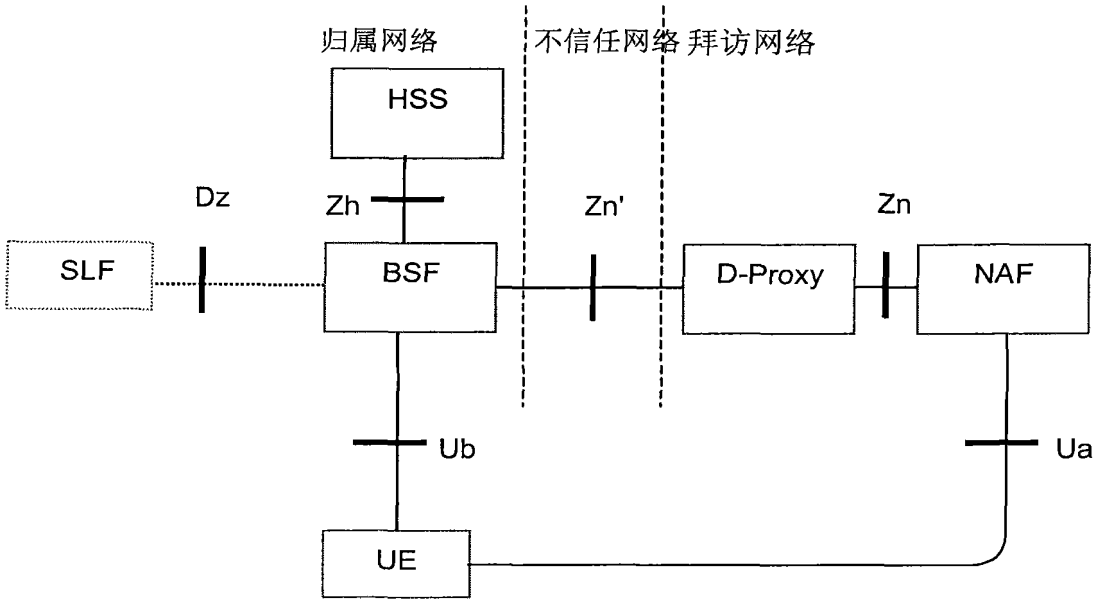
[0483]



[0484] 图 4.1 引导的简单网络模型

[0485] 图 4.1 示出当网络应用功能位于拜访网络中时包含实体的简单网络模型。

[0486]



[0487] 注意 :Zn' 参考点不同于 Zn 参考点,其中它被用在运营商之间。

[0488] 图 4.1a :拜访网络中引导的简单网络模型

[0489] 4.2 网元

[0490] 4.2.1 引导服务器功能 (BSF)

[0491] 通用引导服务器功能 (BSF) 和 UE 应该利用 AKA 协议进行相互认证,并且与后来应用在 UE 和网络应用功能 (NAF) 之间的会话密钥达成协议。BSF 应该通过利用如附录 B 中指定的密钥衍生过程来限制对于特定 NAF 的密钥资料的适用性。密钥衍生过程在密钥资料的生存期期间被用于多个 NAF。根据 BSF 的本地策略设置密钥资料的生存期。在

[0492] 4.5.2 节中指定了密钥资料的生成。

[0493] BSF 应该能够从 HSS 获取 GBA 用户安全设置 (GUSS)。

[0494] BSF 应该能够保持一个列表,其将 NAF 分配到 NAF 组。这个列表用来选择在 GUSS 中哪一个应用专用的 USS 以及是否有应用专用的应用的 USS 对于特定 NAF 是有效的。

[0495] 注意 1 :运营商分配 NAF 到 NAF 组。HSS 中的 NAF 组定义以及所有连接的属于相同运营商网络的 BSF 都应该是相等的。由于这些网元属于相同运营商网络,所以 NAF 组定义自己的标准化在 3GPP 中不是必要的。

[0496] 注意 2 :NAF 分组可以是例如“归属”和“拜访”。它允许 BSF 例如,在归属网络和拜访网络中发送 USS 用于具有例如对于不同 NAF 的不同授权标记的相同应用。例如在拜访网络中,NAF 仅指示请求的应用,但是不会察觉用户的归属网络中的分组。

[0497] 4.2.2 网络应用功能 (NAF)

[0498] 已经完成引导之后,UE 和 NAF 可以运行一些应用专用协议,其中消息的认证将基于 UE 和 BSF 间相互认证期间生成的那些会话密钥。

[0499] 对于 NAF 功能性的通常假设在于 :

[0500] - 在 UE 和 NAF 之间没有先前的安全关联 ;

[0501] -NAF 应该能够定位并且与用户的 BSF 进行安全的通信。

[0502] -NAF 在应用专用协议的运行期间,应该能够获得 UE 和 BSF 之间建立的共享密钥资

料。

[0503] -NAF 应该能够通过 BSF 从 HSS 获得零个或多个应用专用的 USS ;

[0504] -NAF 应该能够根据本地策略设定共享密钥资料的本地有效条件。

[0505] - 在 GBA_U 的情况中,NAF 应该能够通过使用 NAF 中的本地策略或者应用专用 USS 中的密钥选择指示确定应该使用哪个密钥 (即, Ks_ext_NAF 或者 Ks_int_NAF 或者以上两者)。如果 NAF 已经接收了包含密钥选择指示应用专用 USS,则这应该忽略 NAF 中的本地策略

[0506] -NAF 应该能够检测共享密钥资料的生存期和本地有效条件。

[0507] 注意 :没有额外方法的情况下, GBA 不保证密钥的刷新,某种意义上, Ks(_int/ext)_NAF 不保证密钥没有被用于 Ua 协议的之前运行中。UE 和 NAF 可以采取的以保证 GBA 中的密钥刷新的额外的方法是 :

[0508] 1) 在衍生新 Ks_NAF 之前,强制 Ub 协议的新运行。

[0509] 2) 存储以前使用的密钥 Ks(_int/ext)_NAF,或者相应的密钥标识符 B-TID,直到它们生存期结束。

[0510] 支持 Ua 协议 (在协议的无连接运行上不提供回放保护) 的 UE 和 NAF 将需要采取相应行动以避免回放攻击 (如果需要的话)。

[0511] 4.2.2a 直径 (diameter) 协议 (D-Proxy)

[0512] 在其中 UE 已经连接到操作于另一个网络而不是归属网络的 NAF 的情况中,此拜访 NAF 应该使用 NAF 网络的直径协议 (D-Proxy) 以与用户的 BSF(即,归属 BSF) 进行通信。

[0513] 注意 :D-Proxy 功能性可以作为分离的网元来实现,或者作为拜访网络中实现直径代理功能性的任何 NE 的一部分 (这样 NE 的例子是拜访 NAF 所属网络的 BSF 或者 AAA- 服务器)。

[0514] D-Proxy 功能性的一般要求是 :

[0515] D-Proxy 应该能够在拜访 NAF 和用户的归属 BSF 之间起到代理的功能 ;

[0516] D-Proxy 应该能够定位用户的归属 BSF 并且在安全信道上与它通信 ;

[0517] D-Proxy 应该能够验证拜访 NAF 被授权加入 GBA,并且应该能够向用户的归属 BSF 声明拜访的 NAF DNS 名称。D-Proxy 还应该能够向 BSF 声明拜访的 NAF 被授权请求包含在 NAF 请求中的 GBA 特定用户简档。

[0518] D-Proxy 的物理安全级别不应该低于与之接口连接的 NAF 的最高级别。

[0519] 4.2.3 HSS

[0520] 所有用户安全设置的集合 (USS),即 GUSS,存储在 HSS 中。在其中用户具有多个订阅,即 UICC 上的多个 ISIM 或者 USIM 应用的情况中, HSS 应该包含可以映射到一个或者多个私有身份,即 IMPI 和 IMSI 的一个或者多个 GUSS。

[0521] HSS 的要求是 :

[0522] -HSS 应该仅对于 GUSS 提供永久性存储 ;

[0523] -GUSS 应该以这样的方式定义,即对于标准化应用简档不同运营商的交互是可能的。

[0524] -GUSS 应该以这样的方式定义,即不需要这些元素的标准化而支持运营商指定应用的简档和对于现存应用的扩展。

[0525] -GUSS 应该能够包含应用专用 USS，该 USS 包含由一个或者多个 NAF 主持的一个或多个应用的标识或者鉴权信息、GBA_U 情况中的密钥选择指示（即，是否 NAF 应该使用 Ks_ext_NAF 或者 Ks_int_NAF）的相关参数。任何其他类型的参数在应用专用 USS 中不允许。

[0526] 注意 1：可以使用由应用专用 USS 提供的身份信息通过 NAF 直接从 HSS 或者从它的本地数据库中获取必要的用户简档数据。

[0527] 注意 2：如果临时从用户撤销服务，则 HSS 可以从 GUSS 中临时移除这个应用专用 USS。

[0528] -GUSS 应该能够包含针对 BSF 使用的参数：

[0529] - 发布给用户的 UICC 的类型（即是否支持 GBA_U 功能）；

[0530] - 用户特定的密钥生存期。

[0531] - 可选择地，指示 GUSS 已经由 HSS 最后修改的时间的时间戳。

[0532] 注意 3：这些参数是可选的，如果用户的 GUSS 缺少它们或者用户没有 GUSS，那么 BSF 将使用由特别 MNO 定义的 BSF 本地策略中的缺省值。

[0533] HSS 应该能够分配应用专用 USS 到 NAF 组。这将以这样的方式定义，即对于相同应用，但是不同 NAF 组的不同 USS 是可能的。每 GUSS 的 USS 的数量限制依靠通过运营商的 NAF 分组使用。

[0534] - 如果没有针对这个应用定义 NAF 组，那么每个应用最多有一个 USS 存储在 GUSS 中。

[0535] - 如果针对这个应用定义了 NAF 组，那么每个应用最多有一个 USS 和 NAF 组存储在 GUSS 中。

[0536] -HSS 中的 NAF 组定义和所有连接的属于相同运营商网络的 BSF 应该是相等的。

[0537] 4.2.4 UE

[0538] 要求的 UE 功能性是：

[0539] - 支持 HTTP 摘要 AKA 协议；

[0540] - 在引导中使用 USIM 和 ISIM 两者的能力；

[0541] - 当 USIM 和 ISIM 都存在时，选择在引导中使用 USIM 还是 ISIM 的能力；

[0542] - 对于 ME 上的 Ua 应用，向 ME 上的 GBA 功能指示 UICC 应用的类型或者名称以在引导中使用的能力；

[0543] - 从 CK 和 IK 衍生新的将和 Ua 接口上的协议一起使用的密钥资料的能力；

[0544] - 支持 NAF 专用应用协议（例子见 TS 33.221[5]）。

[0545] GBA 察觉的 ME 应该支持如 5.2.1 节中指定的 GBA_U 和 4.5 节中指定的 GBA_ME 两者。

[0546] 4.2.5 SLF

[0547] 该 SLF：

[0548] - 由 BSF 连同 Zh 接口操作查询以得到包含所需用户特定数据的 HSS 的名称。

[0549] - 通过 Dz 接口由 BSF 访问。

[0550] 在单独 HSS 环境中不要求 SLF。当配置 / 管理 BSF 以使用预定义的 HSS 时不要求使用 SLF。

[0551] 4.3 引导架构和参考点

[0552] 4.3.1 参考点 Ub

[0553] 参考点 Ub 处于 UE 和 BSF 之间。参考点 Ub 提供 UE 和 BSF 间的相互认证。它允许 UE 基于 3GPP AKA 基础结构引导会话密钥。

[0554] 指定于 RFC 3310[4] 中的 HTTP 摘要 AKA 协议用在参考点 Ub 上。它是基于 3GPP AKA TS 33.102[2] 协议的。到 USIM 的接口如 TS 31.102[1] 中指定并且到 ISIM 的接口如 TS 31.103[10] 中指定的。

[0555] 4.3.2 参考点 Ua

[0556] 参考点 Ua 承载应用协议，其是利用作为参考点 Ub 上运行 HTTP 摘要 AKA 的结果的 UE 与 BSF 之间协商的密钥资料来保证安全的。例如，在支持用户证书 TS 33.221[5] 情况下，它是允许用户从 NAF 请求证书的协议。在这种情况下，NAF 将是 PKI 入口。

[0557] 4.3.3 参考点 Zh

[0558] 使用于 BSF 和 HSS 之间的参考点 Zh 允许 BSF 从 HSS 获得必要的认证信息和所有的 GBA 用户安全设置。到 3G 认证中心的接口是 HSS 内部的，并且不需要作为此架构的一部分进行标准化。

[0559] 4.3.4 参考点 Zn

[0560] 参考点 Zn 由 NAF 使用以获取之前 HTTP 摘要 AKA 协议从 UE 到 BSF 在参考点 Ub 上运行期间协商的密钥资料。如果其被 NAF 请求，则它也被用于从 BSF 获取应用专用的用户安全设置。

[0561] 4.3.5 参考点 Dz

[0562] 使用于 BSF 和 SLF 之间的参考点 Dz 允许 BSF 获得包含所需用户特定数据的 HSS 的名称。

[0563] 4.4 引导的要求和原理

[0564] 下面的要求与原理可应用于引导过程：

[0565] - 引导功不应该依赖特定的 NAF；

[0566] - 实现引导功能的服务器需要被归属运营商所信任以处理认证向量；

[0567] - 实现 NAF 的服务器仅需要被归属运营商所信任以处理衍生的密钥资料；

[0568] - 在运营商的归属网络和拜访网络中支持 NAF 应该是可能的；

[0569] - 该架构不应该排除在第三网络中对网络应用功能的支持；

[0570] - 在可能的程度上，应该重新利用现存协议和基础设施；

[0571] - 为了确保宽广的适用性，所有相关协议优选运行于 IP 上；

[0572] - 应该阻止正在使用 GBA 的一个 NAF 中的安全漏洞被攻击者用来对使用 GBA 的其它 NAF 实施成功的攻击。

[0573] - 攻击者应该不能够通过 Ua 使用一个安全协议中的漏洞来达到对 Ua 上不同安全协议实施成功的攻击。

[0574] 4.4.1 接入独立性

[0575] 引导过程是接入独立的。引导过程序要来自于 UE 的 IP 连接。

[0576] 4.4.2 认证方法

[0577] 在没有有效的蜂窝订阅的情况下，UE 与 BSF 之间的认证应该是不可能的。认证应该基于 3GPP AKA 协议。

[0578] 4.4.3 漫游

[0579] 漫游的要求：

[0580] - 漫游用户应该能够利用归属网络中的引导功能。用户应该能够利用处于拜访网络中的网络应用功能；

[0581] - 归属网络应该能够控制它的用户是否被授权以使用拜访网络中的服务。

[0582] 4.4.4 参考点 Ub 的要求

[0583] 参考点 Ub 的要求是：

[0584] -BSF 应该能够识别 UE；

[0585] -BSF 和 UE 应该能够基于 AKA 彼此认证；

[0586] -BSF 应该能够发送引导事务标识符到 UE；

[0587] -UE 和 BSF 应该建立共享密钥；

[0588] -BSF 应该能够向 UE 指示密钥资料的生存期。由 BSF 通过 Ub 发送的密钥生存期将指示密钥的到期时间。

[0589] 注意：这并排除 UE 根据 UE 的本地策略在到期时间之前刷新密钥。

[0590] 4.4.5 参考点 Zh 的要求

[0591] 参考点 Zh 的要求是：

[0592] - 相互认证，应该提供保密性和完整性；

[0593] 注意 1：如果 BSF 和 HSS 位于相同运营商网络内，此要求可以通过物理的或者专有的安全方式来满足。

[0594] -BSF 应该能够发送关于用户的引导信息请求；

[0595] - 选择性地，BSF 可以具有能够将用户的 GBA 用户安全设置的时间戳发送到 HSS（时间戳选项）的能力；

[0596] -HSS 应该能够每次发送一个 3GPP AKA 向量到 BSF；

[0597] -HSS 应该能够为了安全目的的需要将用户的 GBA 用户安全设置的完整集合发送到 BSF；选择性地，HSS 可以具有向 BSF 指示 BSF 是否已经基于 GUSS 时间戳（时间戳选项）具有 GUSS 的最新副本的能力。

[0598] 注意 2：如果用户的 GUSS 在 HSS 中进行了更新，则此其不传送至 BSF。作为引导过程的一部分，当 BSF 下次通过 Zh 参考点从 HSS 获取认证向量和 GUSS 的时候，BSF 中的 GUSS 会被更新。

[0599] - 在 HSS 中将不需要关于引导的状态信息；

[0600] - 参考点 Zh 上的所有过程应该由 BSF 初始化的；

[0601] - 到 HSS 的不同接口的数量应该最少。

[0602] 4.4.6 参考点 Zn 的要求

[0603] 参考点 Zn 的要求是：

[0604] - 相互认证，应该提供保密性和完整性；

[0605] 如果 BSF 和 NAF 位于相同的运营商的网络内，则 Zn 参考点应该根据 NDS/IP[13] 受到保护；

[0606] - 如果 BSF 和 NAF 位于不同的运营商的网络中，在 D-Proxy 和 BSF 之间的 Zn’参考点应该使用如 RFC 2246[6] 中指定的 TLS 来保证安全；

[0607] 注意 1 :附录 E 指定 TLS 简档用于保证 Zn' 参考点的安全。

[0608] -BSF 应该验证请求 NAF 被授权以获得密钥资料或者密钥资料和被请求的 USS ;

[0609] -NAF 应该能够发送密钥资料请求到 BSF,包含由 UE 的相应请求使用的 NAF 的公共主机名。BSF 应该能够验证 NAF 被授权以使用此主机名,即,当它联系 NAF 时,UE 使用的 FQDN ;

[0610] -BSF 应该能够发送密钥资料到 NAF ;

[0611] -NAF 应该能够根据 BSF 的策略以及来自于 Zn 上的 NAF 的请求中指示的应用从 BSF 获得应用专用 USS 选择的集会 ;

[0612] -NAF 应该能够向 BSF 指示其需要 USS 所针对的单个应用或几个应用 ;

[0613] 注意 2 :如果一些应用只需要应用专用的 USS 的子集,例如,仅一个 IMPU,则 NAF 从发送自 BSF 的完整 USS 集合中选择这个子集。

[0614] - 如果私有用户身份和应用专用的 USS 可以被发送至 NAF,则 BSF 应该能够在每个 NAF 或每个应用的基础之上配置 ;

[0615] 注意 3 :如果 BSF 没有将 IMPI 或者 USS 中的任何其它用户身份发送到 NAF,则用户向 NAF 保持匿名 ;或者更精确地,B-TID 功能作为临时用户假名。

[0616] - 如果 NAF 向 BSF 请求 USS 并且它们没有出现在用户的 GUSS 中,它不应引起一个错误,假设满足提供的 BSF 本地策略的条件。然后,BSF 应该仅将请求的和发现的 USS 发送到 NAF ;

[0617] - 如下配置本地策略是可能的 :BSF 可以要求一个或者多个应用专用的 USS 存在于用于特定的请求 NAF 的特定用户的 GUSS 中,并且如果不满足条件,则拒绝来自于 NAF 的请求。为了满足这个本地策略,NAF 不需要通过 Zn 参考点请求 USS,BSF 要求其存在于 GUSS 中,更确切地说 BSF 检查 USS 的本地存在已经足够了。以没有 USS 被要求用于请求 NAF 这样的方式配置 BSF 是可能的 ;

[0618] 注意 4 :关于本地策略使用的更多信息,见附录 J

[0619] -BSF 应该能够向 NAF 指示引导的时间和密钥资料的生存期。由 BSF 通过 Zn 发送的密钥生存期应该指示密钥的到期时间,并且应该与由 BSF 通过 Ub 发送到 UE 的密钥的生存期一致。

[0620] 注意 5 :这不能排除 NAF 根据 NAF 的本地策略在到期时间之前刷新密钥。

[0621] 注意 6 :如果一个或者多个已经发送到 NAF 的 USS 已经在 HSS 中的用户 GUSS 中更新了,则此变化在下次它通过 Zn 参考点从 BSF 获取 USS 时告知 NAF(假设 BSF 已经通过 Zh 参考点从 HSS 更新了用户的 GUSS)。

[0622] 4.4.7 引导事物标识符的要求

[0623] 引导事务标识符 (B-TID) 应该用于将用户身份绑定到参考点 Ua, Ub 和 Zn 中的密钥资料。

[0624] B-TID 的要求是 :

[0625] -B-TID 应该是全局唯一的 ;

[0626] -B-TID 应该在参考点 Ua 中使用的协议内可用作密钥标识符 ;

[0627] -NAF 应该能够从 B-TID 中检测 UE 的归属网络和 BSF。

[0628] 注意 1 :密钥已经无效之后,NAF 可以基于删除条件移除安全关联。

[0629] 注意 2 :不得不注意 UE 和 NAF 之间的 GBA 和非 GBA 认证的并行使用例如,在命名空间中不导致冲突。这种潜在的冲突不能以通用的方式解决,因为它依靠于 UE 和应用服务器之间使用的特定协议和认证机制。因此,它处于本规范的范围之外。

[0630] 对于 UE 和 NAF 之间使用的 HTTP 摘要认证的例子,如下应用的并行使用是可能的 :<用户名,密码 > 对对于仅一个域必须是唯一的。由于 NAF 控制域名,所以它必须确保只有基于 GBA 的域才能以保留的 3GPP 域名命名。在 NAF 希望允许基于非 GBA 的认证也处于 GBA 域中的特殊的情况下,它必须确保没有 B-TID 格式的用户名被用在基于 GBA 的认证之外。

[0631] 4.4.8 UICC 应用的选择和相关密钥的要求

[0632] 当几个应用存在于 UICC 之上时,它们能够运行 AKA,那么 ME 应该选择这些 UICC 应用的一个用于以下列优选项顺序执行本文档中规定的 GBA 的过程 :

[0633] 1. UE 确定包括哪个 UICC 应用 :

[0634] a. ME 上需要 Ks_NAF 的应用 (Ua 应用) 可以向 GBA 支持功能 (GBA 功能) 指示 UICC 应用的类型或名字 :没有优先级,USIM,ISIM,或者 UICC 应用的“标签”(见 TS 31.101[15] 中的定义)。

[0635] 如果 ME 上的应用指示 UICC 应用的“标签”,则执行下面的步骤 b。

[0636] 如果 ME 上的应用指示 UICC 应用的类型应该是 :

[0637] -UICC 上的 USIM ;略过下面的步骤 b 并且在步骤 c 和 d 中的仅考虑 USIM 应用。

[0638] -UICC 上的 ISIM ;略过下面的步骤 b,并且在步骤 c 和 d 中的仅考虑 ISIM 应用。

[0639] 如果 ME 上的应用没有指示优选项,则略过下面的步骤 b 并且如下描述,从步骤 c 开始执行选择过程。

[0640] b. 如果在步骤 a 中指示了“标签”,则 GBA 功能应该选择 (见 TS31.102[1] 中的定义) 具有指示的“标签”的 UICC 应用 ;如果此 UICC 应用的选择不成功,则选择过程失败。

[0641] c. 如果在步骤 a 中没有指示“标签”,则 GBA 功能应该在激活的 UICC 应用中选择 ;如果存在多于一个的激活的 UICC 应用,则 GBA 功能可以向终端用户示出选择对话的 UICC 应用 (该列表包含来自于 UICC 应用列表的“标签”),从中终端用户可以选择将要被选择的 UICC 应用 ;如果没有示出会话,则 GBA 功能应该选择“上次选择的”活动的 UICC 应用 ;如果 Ua 应用指示了“无优先级”并且“上次选择的”USIM 和“上次选择的”ISIM 处于活动状态,那么“上次选择的”USIM 被选择。

[0642] d. 如果不存在活动的 UICC 应用 :

[0643] - 如果仅存在一个 UICC 应用,如果可能,则 GBA 功能选择它 ;

[0644] - 如果存在多于一个的 UICC 应用,则 GBA 功能可以向终端用户示出选择对话的 UICC 应用 (该列表包含来自于 UICC 应用列表的“标签”),从中终端用户可以选择将被选择的 UICC 应用。如果没有示出会话,如果肯能,则 GBA 功能应该选择“上次选择的”UICC 应用 ;

[0645] e. 如果指示于步骤 a 中并且使用于步骤 d 中的类型是 ISIM,但是不存在 ISIM 供选择,那么使用类型 USIM 重复步骤 d ;否则选择过程失败。

[0646] 注意 1 :步骤 e 被要求用于下列情况 :可以使用 UICC 上的 USIM 应用来认识如 TS 33.203[16] 中定义的 ISIM。

[0647] 2. 如果已经存在从 UICC 应用衍生的密钥 Ks,则 UE 采用此密钥以衍生 Ks_NAF。

[0648] 3. 如果不存在这样的密钥 Ks，则 UE 首先运行包含选择的 UICC 应用的 Ub 协议，然后到步骤 2。

[0649] 如果选择了 USIM，则从如 TS 22.003[11]13.3 节中指定的那样存储在 USIM 上的 IMSI 获得的 IMPI 被用于运行在 Ub 上的协议中。

[0650] 注意 2：严格地讲，IMPI，以及如 TS23.003[11] 来自于 IMSI 的 IMPI 的衍生仅在 IMS 的上下文中定义。然而，出于规范的目的，如 TS23.003[11]13.3 章中指定的从 IMSI 获得的标识符也称为 IMPI，即使用户没有 IMS 订阅。

[0651] 如果选择了 ISIM，则储存在 ISIM 上的 IMPI 被用于运行在 Ub 上的协议中。

[0652] 不论何时 UICC 应用被成功地选择或者终止，用于选择 UICC 应用的本节中的规则是重复应用的，并且因此，为 GBA 选择的 UICC 应用可以改变。

[0653] 不论何时 UICC 应用被终止，则通过 Ub 参考点（根据 4.5.2 和 5.3.2 节）在协议中从其建立的共享密钥 Ks 应该被删除。

[0654] 注意 3：在任一时刻，最多存在一个 UICC 应用，用于执行 GBA 过程。

[0655] 注意 4：在直到密钥的生存期到期，在共享密钥 Ks 已经被删除之后，Ua 应用可以继续使用衍生的 NAF 特定密钥 (Ks_(ext/nt)_NAF)。

[0656] 4.4.9 参考点 Ua 的要求

[0657] 参考点 Ua 的一般要求是：

[0658] -UE 和 NAF 应该能够使用基于 GBA 的共享秘密保证参考点 Ua 的安全；

[0659] 注意 1：保证参考点 Ua 安全的确切方法依靠参考点 Ua 上使用的应用协议。

[0660] - 在 GBA_U 的情况中，UE 和 NAF 应该能够就密钥（即，Ks_ext_NAF 或者 Ks_int_NAF 或者以上两者）达成一致，作为基于 GBA 的共享秘密使用，如果两个密钥可以被使用。

[0661] 注意 2：有两种方式在 UE 和 NAF 之间就使用哪个密钥 (Ks_(ext) 或 Ks_int 或二者）达成一致：

[0662] 1) 在一般情况中，其中在参考点 Ua 上使用的协议可以被用于不同应用（例如，HTTPS)，协议应该能够指示应该使用哪个密钥。

[0663] 2) 在特定应该中，其中协议是应用专用的（流入，MBMS 中的 MIKEY)，协商可以基于隐性知识。

[0664] -Ua 上的任何安全协议应该关联于 Ua 安全协议标识符。此标识符将指定于此规范的附录 H 中。

[0665] -NAF 应该能够向 UE 指示应该使用的基于 GBA 的共享秘密；

[0666] -NAF 应该能够向 UE 指示已经到期的当前共享秘密并且 UE 应该与 NAF 使用较新的共享秘密。

[0667] - 当在 Ua 应用规范中没有指定时，NAF 专用密钥资料 Ks_(ext/int)_NAF 的默认生命期应该等于 Ks 的生命期。Ks_(ext/int)_NAF 的默认生命期应该不超过于相应的 Ks 的生命期。

[0668] -UE 和 NAF 可以使密钥资料 Ks_(ext/int)_NAF 适应参考点 Ua 的特定需要。此适应处于此规范的范围之外。当在 Ua 应用规范中没有指定时，适应的密钥资料的默认生命期应该等于 Ks_(ext/nt)_NAF 的生命期。适应的密钥资料的生命期不应该超过相应 Ks_(ext/int)_NAF 的生命期。

[0669] 4.4.10 参考点 Dz 的要求

[0670] BSF 和 SLF 之间的这个接口被用于检索保持给定用户的订阅的 HSS 的地址。在单个 HSS 环境中此接口不是必需的。

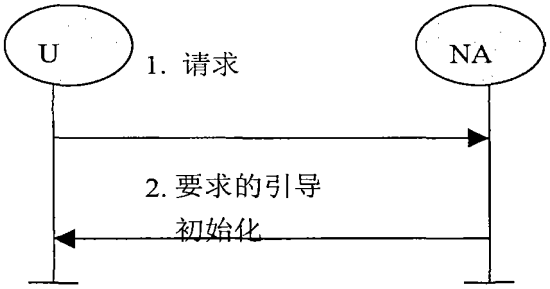
[0671] 4.5 过程

[0672] 这一节详细指定由不同应用进一步利用的引导过程的格式。它包含使用 BSF 的 AKA 认证，以及密钥资料的产生过程。

[0673] 4.5.1 引导的初始化

[0674] 在 UE 和 NAF 间的通信可以开始之前，UE 和 NAF 首先必须协商是否使用 GBA。当如果 UE 希望与 NAF 交互时，但是它不知道 NAF 是否需要使用通过 GBA 方式获得的共享密钥，这时，UE 应该为了进一步指示联系 NAF（见图 4.2）。

[0675]



[0676] 图 4.2：引导的初始化

[0677] 1. UE 通过参考点 Ua 发起与 NAF 的通信而没有任何 GBA 相关参数。

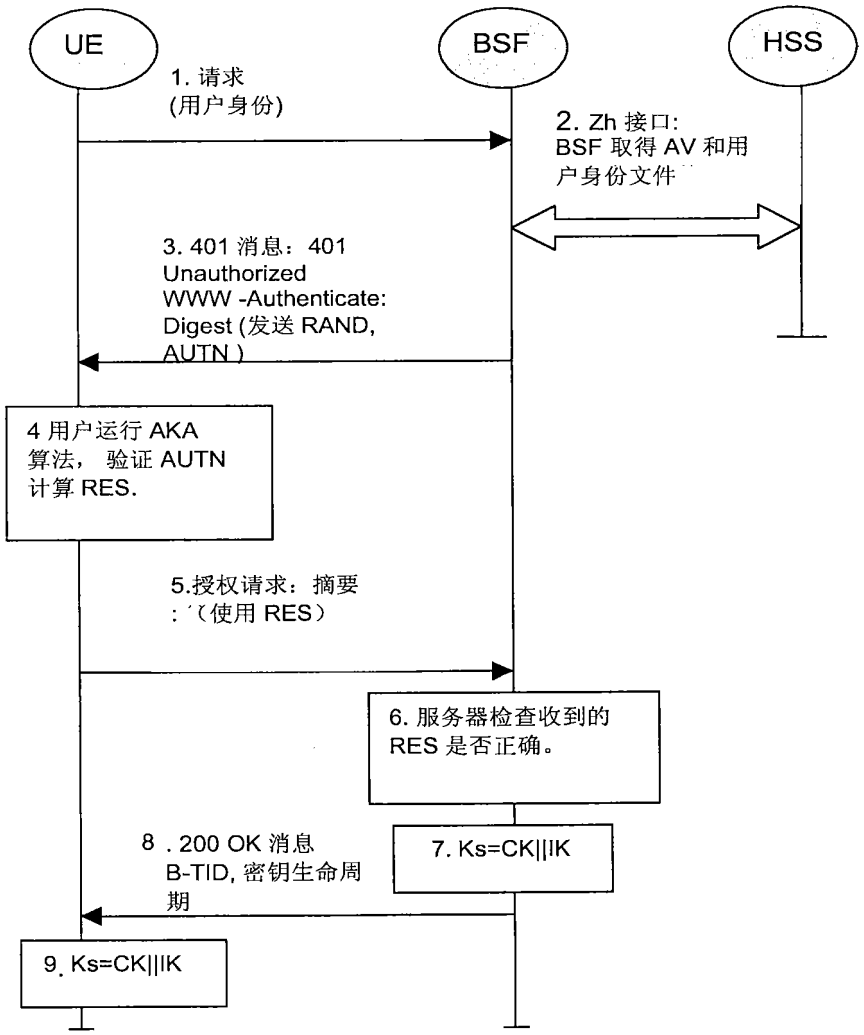
[0678] 2. 如果 NAF 需要使用通过 GBA 方式获得的共享密钥，但是来自 UE 的请求中不包括 GBA 相关参数，则 NAF 使用引导初始化信息进行回复。这种指示方式可以依靠于特定的参考点 Ua 并且在相关的阶段 3 规范中指定。

[0679] 4.5.2 引导过程

[0680] 当 UE 希望与 NAF 交互，并且它知道需要引导过程时，它将首先执行引导认证（见图 4.3）。否则，仅当它已经接收到引导初始化要求消息或者来自 NAF 的引导协商指示时，或者当 UE 中的密钥生存期已经到期时，UE 应该执行引导认证。（协议 4.5.3 子节）。

[0681] 注意 1：来自于规范 TS 33.102[2] 的 AKA 协议以及 RFC 3310[4] 中的 HTTP 摘要 AKA 协议中的主要的步骤为了读者的方便在图 3 中重复。假如存在任何潜在的冲突，以 TS 33.102[2] 和 RFC 3310[4] 中的规范优先。

[0682]



[0683] 图 4.3 引导过程

[0684] 1.UE 向 BSF 发送 HTTP 请求。

[0685] 2.BSF 通过参考点 Zh 从 HSS 检索 GBA 用户的安全设置的完整集合和一个认证向量 (AV, AV = RAND || AUTN || XRES || CK || IK)。

[0686] 如果 BSF 实现时间戳选项并且具有在以前引导过程期间从 HSS 已经获得的用户的 GUSS 的本地副本，并且此 GUSS 包括时间戳，则 BSF 可以在请求消息中包括 GUSS 时间戳。当接收那个时间戳时，如果 HSS 实现了时间戳选项，则 HSS 可以将其与存储在 HSS 中的 GUSS 时间戳比较。在此情况中，如果并且仅如果 HSS 已经完成比较并且时间戳是相等的，那么 HSS 应该发送“GUSS 时间戳相等”指示到 BSF。在任何其他情况中，HSS 应该发送 GUSS（如果有效）到 BSF。如果 BSF 接收到“GUSS 时间戳相等”的指示，它将保留 GUSS 的本地副本。在任何其他情况中，BSF 应该删除 GUSS 的本地副本，并且存储接收的 GUSS（如果发送了）。

[0687] 注意 2 :在多个 HSS 的环境中，BSF 不得不获取 HSS 的地址，其中在步骤 2 之前，通过查询 SLF 存储用户的订阅。

[0688] 3. 然后，BSF 在 401 消息中将 RAND 和 AUTN（没有 CK、IK 和 XRES）转发到 UE。这是要求 UE 认证自己。

[0689] 4.UE 检查 AUTN 以验证质询来自于授权网络 ;UE 还计算出 CK，IK 和 RES。这将导

致会话密钥 IK 和 CK 在 BSF 和 UE 两者中。

[0690] 5. UE 发送另一个包含摘要 AKA 响应（使用 RES 计算）的 HTTP 请求到 BSF。

[0691] 6. BSF 通过验证摘要 AKA 响应来对 UE 进行认证。

[0692] 7. BSF 通过连接 CK 和 IK 来生成密钥资料 Ks。通过采用来自于步骤 3 的 base64 编码的 [12]RAND 值和 BSF 服务器名，即 base64encode(RAND)@BSF_servers_domain_name 以 NAI 的格式生成 B-TID 值。

[0693] 8. BSF 应发送包括 B-TID 的 200 OK 消息到 UE 以指示认证成功。另外，在这个 200 OK 消息中，BSF 应该提供密钥 Ks 的生存期。在 UE 中通过连接 CK 和 IK 生成密钥资料 Ks。

[0694] 9. 在如 4.5.3 节中指定的过程期间，UE 和 BSF 两者都应该使用 Ks 以衍生密钥资料 Ks_NAF。Ks_NAF 应该用于保证参考点 Ua 的安全。

[0695] 如以 Ks_NAF = KDF(Ks, " gba-me" ,RAND,IMPI,NAF_Id) 计算 Ks_NAF，其中 KDF 是附录 B 中定义的密钥衍生函数，并且密钥衍生参数由用户的 IMPI、NAF_Id 和 RAND 组成。NAF_Id 由 NAF 的全 DNS 名组成，与附录 H 中指定的 Ua 安全协议标识符连接。KDF 应该在 ME 中实现。

[0696] 注意 3：为了允许基于 UE 和 BSF 中 NAF 名称的一致密钥衍生，应满足下列三个前提条件中的至少一个：

[0697] (1) 在 DNS 中，NAF 仅在一个域名下 (FQDN) 是已知的，即，没有两个不同域名指向 NAF 的 IP 地址。这必须通过管理方式完成。这个前提条件不指定于 3GPP，因为在其他环境下也是必须的，例如对于没有使用通配符 (wildcard) 或多名证书的 TLS V1.0。

[0698] (2)NAF 的每个 DNS 入口指向不同的 IP 地址。NAF 响应所有这些 IP 地址。每个 IP 地址通过 NAF 配置绑定到相应的 FQDN。NAF 可以从 IP 地址看到哪个 FQDN 用于密钥衍生。

[0699] (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报头字段的 HTTP/1.1）。这需要 NAF 检查主机名的有效性，在与适当 UE 的所有通信中使用这个名字，并且将这个名字传送给 BSF 以允许 Ks_NAF 的正确衍生。

[0700] 在 TLS 隧道的情况下，这需要多身份证书或 RFC 3546[9] 或者带有类似目的的其他的协议方法的部署。

[0701] UE 和 BSF 应该存储带有相关 B-TID 的密钥 Ks 用于将来的使用，直到 Ks 的生存期已经到期，或者直到密钥 Ks 被更新。

[0702] 4.5.3 使用引导安全关联的过程

[0703] 在 UE 和 NAF 可以开始通信之前，UE 和 NAF 首先必须协商是否使用通过 GBA 方式获得的共享密钥。如果 UE 不知道是否与 NAF 使用 GBA，则它使用 4.5.1 节中描述的引导初始化过程。

[0704] 一旦 UE 和 NAF 已经建立它们希望使用的 GBA，那么每次 UE 希望与 NAF 交互，则执行图 4.4 中描述的下列步骤。

[0705] 1. UE 通过参考点 Ua 与 NAF 开始通信：

[0706] - 通常，UE 和 NAF 将尚未共享要求的密钥以保护参考点 Ua。如果它们已经共享了该密钥（即，如果用于相应的密钥衍生参数 NAF_Id 密钥 Ks_NAF 已经是有效的），则 UE 和 NAF 就可以立刻开始安全的通信。如果 UE 和 NAF 还没有共享密钥，UE 如下继续执行：

[0707] - 如果 UE 中用于选择的 UICC 应用的密钥 Ks 是有效的，则如 4.5.2 节制定的 UE 从

Ks 衍生密钥 Ks_NAF ;

[0708] - 如果 UE 中没有用于选择的 UICC 应用的密钥 Ks 是有效的，则 UE 首先通过参考点 Ub 与 BSF 就新密钥 Ks 达成一致，并且然后进行衍生 Ks_NAF 的过程 ;

[0709] 注意 1 :如果对于 UE 来说不希望使用用于被选的 UICC 应用的相同 Ks 密钥来衍生出多于一个 Ks_NAF，那么 UE 就应该首先通过参考点 Ub 与 BSF 就新的密钥 Ks 达成一致，然后进行衍生 Ks_NAF 的过程。

[0710] - 如果 NAF 与 UE 共享密钥，但是 NAF 要更新该密钥，例如，因为密钥的生存期已经到期或者很快将到期，或者该密钥不能满足 NAF 本地有效条件，则它将发送合适的引导的重协商请求到 UE，见图 4.5。如果密钥的生存期已经到期，则参考点 Ua 上使用的协议将被终止。这个指示的形式依靠参考点 Ua 上使用的特定协议。如果 UE 接收了引导重认证请求，则它为了获得新密钥 Ks，如 4.5.2 节指定的，开始参考点 Ub 上协议的的运行。

[0711] 注意 2 :为了允许 UE 和 BSF 中的一致密钥衍生，两者都必须使用相同的 FQDN 进行衍生 (见 4.5.2 节的注意 2)。如果只有 4.5.2 节的注意 1 的 (1) 和 (2) 被允许用于 NAF，或者如果在 Ua 上使用的协议也将通过 UE 用于密钥衍生的 FQDN 传送到 NAF，则对于每个使用在 Ua 上的协议，它将被指定。

[0712] 注意 3 :如果 UE 和 NAF 之间的共享密钥是无效的，则 NAF 就可以为后续删除设置相应安全关联的删除条件。

[0713] -UE 以 4.3.2 节中指定的格式向 NAF 提供 B-TID，以允许 NAF 从 BSF 获取相应的密钥。

[0714] 注意 4 :UE 可以使密钥资料 Ks_NAF 适应参考点 Ua 的特定需要。此适应在本规范的范围之外。

[0715] -ME 中 GBA 相关密钥的密钥管理 (即 Ks 和 Ks_NAF) :

[0716] - 当插入不同 UICC 时，所有 GBA 相关密钥应该从 ME 删除。因此 ME 需要在非易失性存储器中存储最新插入的 UICC 身份以能够将其与在 UICC 插入和打开电源时使用的 UICC 身份进行比较。

[0717] -ME 关闭电源时，密钥 Ks 应该从 ME 删除。

[0718] -ME 关闭电源时，所有其他 GBA 相关密钥可从 ME 删除。如果 ME 没有在关闭电源时删除 GBA 密钥，那么 GBA 密钥需要保存在非易失性存储器中。

[0719] - 当通过参考点 Ub 就新 Ks 达成一致并且衍生于一个 NAF_Id 的密钥 Ks_NAF 被更新时，衍生于不同 NAF_Id 并存储在 UE 上的其他 Ks_NAF 将不会受到影响。

[0720] 注意 5 :根据 4.5.2 节和 4.5.3 节中定义的过程，在 UE 中存在每 NAF_Id 最多一个存储的 Ks_NAF。

[0721] 2. NAF 通过参考点 Zn 与 BSF 开始通信，

[0722] -NAF 请求对应于由 UE 通过参考点 Ua 提供给 NAF 的 B-TID 的密钥资料。如果 NAF 具有几个可以与本规范联合使用的 FQDN，那么 NAF 应该通过 Zn 在请求中传输用在 Ua 上的相同 FQDN(见本节中关于密钥衍生的注意 2) ;

[0723] -UE 也可以请求一个或者多个应用专用 USS 用于应用，其通过 Ua 从 UE 接收的请求可以访问 ;

[0724] - 通过密钥资料请求，NAF 将提供 UE 已经使用去访问 NAF 的公共主机名到 BSF，并

且 BSF 将能够验证该 NAF 被授权使用该主机名。

[0725] 3. BSF 从密钥 Ks 和密钥衍生参数中衍生出对在参考点 Ua 上使用的协议进行保护所要求的密钥，如 4.5.2 节中指定的，并且如果在用户 GUSS 中它们是有效的并且如果 NAF 被授权接收所请求的 USS，则向 NAF 提供请求的密钥 Ks_NAF 以及引导时间和密钥的生存期，以及请求的应用专用 USS 和潜在的 NAF 组专用 USS。如果由 NAF 所提供的 B-TID 所标识的密钥在 BSF 是无效的，则 BSF 将对 NAF 的回复中指示。那么，NAF 向 UE 指示引导重协商请求。

[0726] 注意 6 :NAF 可以根据本地策略，例如 Ks_NAF 重用次数限制，来进一步设置 Ks_NAF 的本地有效条件。

[0727] 注意 7 :NAF 将使用与 UE 同样的方式使 Ks_NAF 适应于参考点 Ua 的特定需要。该适应在本规范的范围之外。

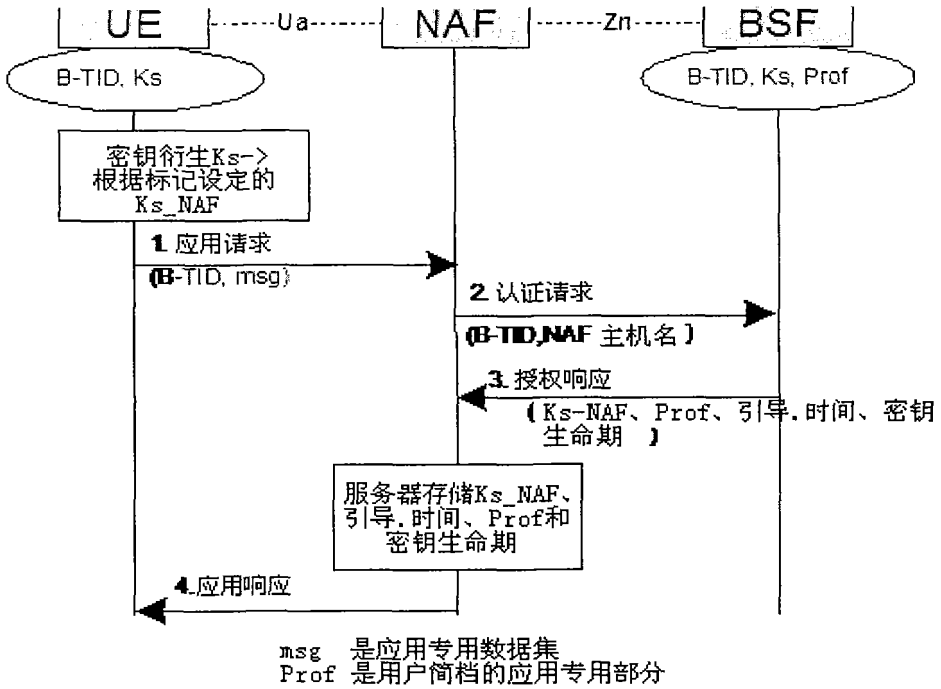
[0728] -BSF 可以要求在用户的 GUSS 内存在用于 NAF 的一个或多个应用专用以及潜在的 NAF 组专用 USS（见 4.4.6 节）。如果 GUSS 缺少一个或多个这些要求的设置，则 BSF 将在对 NAF 的回复中指示这一点。

[0729] -BSF 还可能根据 BSF 的策略将私有用户标识（IMPI）和所请求的 USS 发送给 NAF。

[0730] 4. NAF 通过参考点 Ua 上使用的协议继续与 UE 交互。

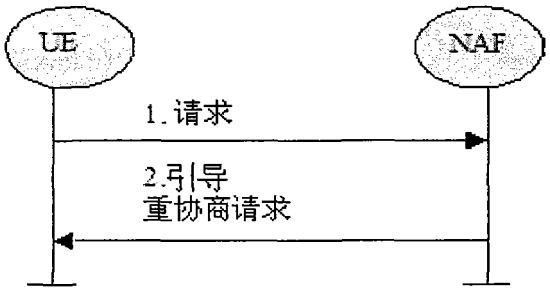
[0731] 一旦在参考点 Ua 上使用协议的运行完成，则达到了引导的目的，因为它使 UE 和 NAF 能够以安全的方式使用参考点 Ua。

[0732]



[0733] 图 4.4 引导使用过程

[0734]



[0735] 图 4.5 :引导重协商请求

[0736] 4.5.4 涉及服务发现的过程

[0737] UE 应该从 UICC 应用相关身份信息发现 BSF 的地址 (UICC 应用在引导过程期间使用) 既,用于 USIM 的 IMSI 或用于 ISIM 的 IMPI。BSF 的地址如 3GPP TS 23.003[11] 中指定的被衍生。5 基于 UICC 的增强的通用引导架构 (GBA U)

[0738] 假设本节指定的过程中包括的 UICC, BSF 和 HSS 能够处理 GBA_U 特定增强。如果 NAF 不是 GBA_U 察觉的,本节中指定的也可以应用。

[0739] 5.1 用于带有基于 UICC 增强的引导的架构和参考点

[0740] 本规范的 4.4 节的文本也应用于此,另外 ME 与 UICC 之间的接口如 TS 31.102[1] 和 TS 31.103[10] 中定义的需要使用 GBA_U 特定命令增强。这些命令的要求可以在 5.2.2.1 中找到,过程的细节在 5.3 节中。

[0741] 5.2 带有基于 UICC 增强的引导的要求和原理

[0742] 4.3 节的要求和原理也应用于此并且带有下列附加内容 :

[0743] 5.2.1 UE 的要求

[0744] Ub 上参考点的协议运行产生的 3G AKA 密钥 CK 和 IK 不应该离开 UICC。

[0745] UICC 应该能够在针对 GBA_U 的认证请求和针对其他 3G 认证域的认证请求间进行区分。

[0746] 在认证请求来自 ME 时 (UICC 知道其与 GBA_U 相关)UICC 应该衍生引导密钥。

[0747] 在请求来自 ME 时,UICC 应该能够从存储在 UICC 上的衍生密钥进一步衍生 NAF 专用的密钥。

[0748] 所有 GBA 察觉的 ME 应该支持前面两种请求的过程。

[0749] 5.2.2 BSF 的要求

[0750] BSF 应该支持 GBA_U 和 GBA_ME 两种引导过程。关于运行一个或其他的决定应该基于订阅信息 (即 UICC 能力)。

[0751] BSF 应该能够从 HSS 获取作为 GBA 用户安全设置的一部分的 GBA 相关的 UICC 能力。

[0752] 5.3 带有基于 UICC 增强的引导的过程

[0753] 5.3.1 引导的初始化

[0754] 本文档的 4.5.1 节的文本也应用于此。

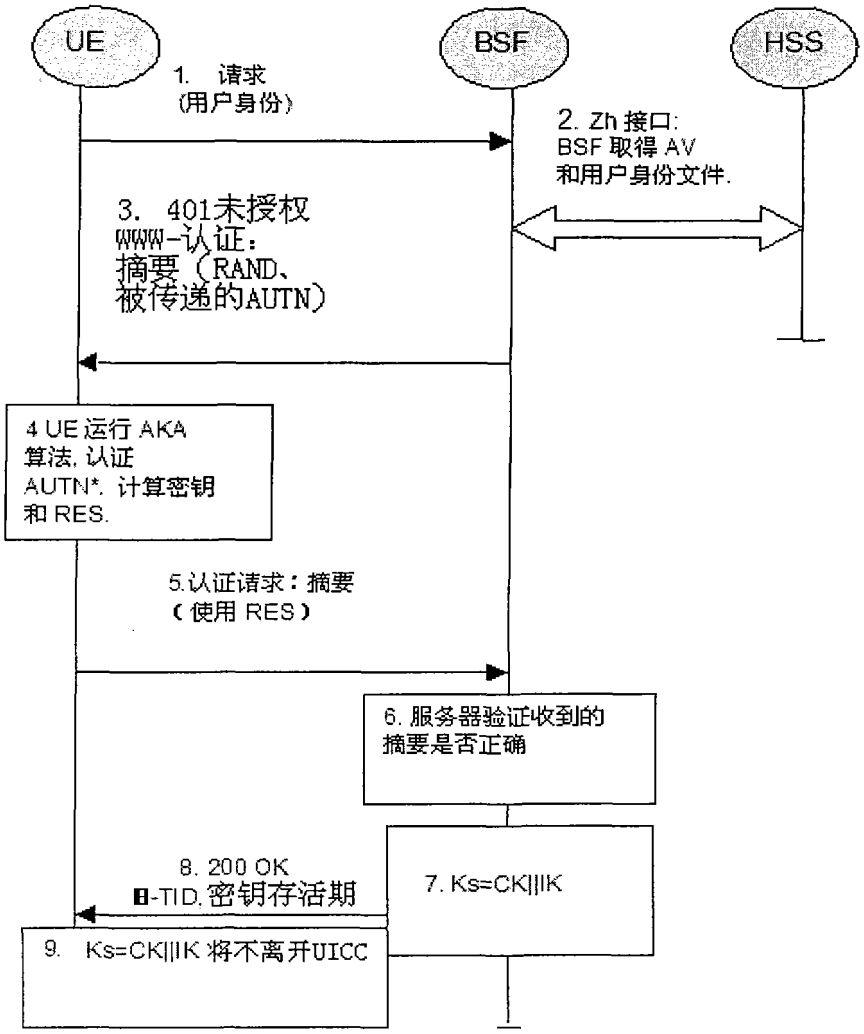
[0755] 5.3.2 引导过程

[0756] 在本节中指定的过程不同于 UE 和 BSF 中密钥和认证向量的本地处理中 4.5.2 节指定的过程。通过 Ub 参考点交换的消息对于两个过程是一致的。

[0757] 当 UE 要与 NAF 进行交互，并且它知道需要引导过程时，则它将首先执行引导认证（见图 5.1）。否则，仅当 UE 已经接收到来自 NAF 的要求引导初始化消息或者引导重认证指示时，或者当 UE 内的密钥生存期已经到期时，UE 将执行引导认证。

[0758] 注意：为了方便读者，TS 33.102[2] 中 AKA 协议的规范和 RFC 3310[4] 中的 HTTP 摘要 AKA 协议的规范的主要步骤在图 5 中重复。如果存在任何潜在冲突，TS 33.102[2] 和 RFC 3310[4] 中的规范优先。

[0759]



[0760] 图 5.1 带有 UICC 增强的引导过程

[0761] 1. ME 向 BSF 发送 HTTP 请求。

[0762] 2. BSF 通过 Zh 参考点从 HSS 获得 GBA 用户安全设置和一个认证向量 (AV，AV = RAND ‖ AUTN ‖ XRES ‖ CK ‖ IK)。

[0763] 如果 BSF 实现时间戳选项并且具有在以前引导过程期间从 HSS 已经获得的用户的 GUSS 的本地副本，并且此 GUSS 包括时间戳，则 BSF 可以在请求消息中包括 GUSS 时间戳。当接收那个时间戳时，如果 HSS 实现了时间戳选项，则 HSS 可以将其与存储在 HSS 中的 GUSS 时间戳进行比较。在此情况中，如果并且仅如果 HSS 已经完成比较并且时间戳是相等的，那么

HSS 应该发送“GUSS 时间戳相等”指示到 BSF。在任何其他情况中，HSS 应该发送 GUSS（如果有效）到 BSF。如果 BSF 接收“GUSS 时间戳相等”的指示，它将保留 GUSS 的本地副本。在任何其他情况中，BSF 应该删除 GUSS 的本地副本，并且存储接收的 GUSS（如果发送了）。

[0764] 然后，BSF 可以基于用户安全设置 (USS) 决定执行 GBA_U。在此情况下，BSF 按照以下方式来进行：

[0765] -BSF 计算 MAC* = MAC ⊕ Trunc(SHA-1(IK))

[0766] 注意 1：Trunc 表示在 SHA 1[21] 所输出的 160 比特中，编号为 [0] 到 [63] 的 64 比特用在对 MAC 的 * 操作中。

[0767] BSF 在去掉 (flip) 最低有效位后，存储 XRES。

[0768] 注意 2：在多个 HSS 环境中，在步骤 2 之前，BSF 必须通过查询 SLF 获得其中存储用户的订阅的 HSS 的地址。

[0769] 3. BSF 将 RAND 和 AUTN*（其中 AUTN* = SQN ⊕ AK ‖ AMF ‖ MAC*）在 401 消息中转发给 UE（没有 CK、IK 和 XRES）。这需要 UE 认证自己的要求。

[0770] 4. ME 将 RAND 和 AUTN* 发送到 UICC。UICC 计算 IK 和 MAC（通过执行 MAC = MAC* ⊕ Trunc(SHA-1(IK))）。然后 UICC 通过检查 AUTN（即 SQN ⊕ AK ‖ AMF ‖ MAC）以验证该质询来自于授权网络；UICC 也计算出 CK 和 RES。这将导致会话密钥 CK 和 IK 在 BSF 和 UICC 两者中。然后 UICC 将 RES（去掉最低有效位后）传输到 ME 并且存储 Ks，其是 UICC 上 CK 和 IK 的串接。

[0771] 5. ME 发送另外一个包含摘要 AKA 响应（利用 RES 计算）的 HTTP 请求到 BSF。

[0772] 6. BSF 通过验证摘要 AKA 来响应认证 ME。

[0773] 7. BSF 通过连接 CK 和 IK 生成密钥 Ks。通过采用来自于步骤 3 的 base64 编码的 RAND 值以 NAI 的格式生成 B-TID 值以及 BSF 服务器名，即，base64encode(RAND)@BSF_servers_domain_name。

[0774] 8. BSF 将向 UE 发送包含 B-TID 的 200 OK 消息以指示认证的成功。另外，在这个 200 OK 消息中，BSF 将提供密钥 Ks 的生存期。

[0775] 9. 如果可应用，UICC 和 BSF 两者将会在 5.3.3 节中指定的过程期间使用 Ks 衍生 NAF 专用密钥 Ks_ext_NAF 和 Ks_int_NAF。Ks_ext_NAF 和 Ks_int_NAF 被用于保证 Ua 参考点的安全。

[0776] Ks_ext_NAF 在 UICC 中以 Ks_ext_NAF = KDF(Ks, " gba-me", RAND, IMPI, NAF_Id) 计算，并且 Ks_int_NAF 在 UICC 中以 Ks_int_NAF = KDF(Ks," gba-u,RAND,IMPI,NAF_Id) 计算，其中 KDF 是附录 B 中指定的密钥衍生函数，并且密钥衍生参数包括用户的 IMPI、NAF_Id 和 RAND。与附录 H 中指定的 Ua 安全协议标识符连接的 NAF_Id 由 NAF 的全 DNS 名组成。用于 Ks_ext_NAF 衍生的密钥衍生参数必须与那些用于 Ks_int_NAF 衍生的不同。这通过在 Ks_ext_NAF 中添加静态字符串" gba-me" 并且在 Ks_int_NAF 中添加静态字符串" gba-u" 作为到衍生函数的输入参数来完成。

[0777] 注意 3：4.5.2 节的注意 3 同样应用于此。

[0778] UICC 和 BSF 为了能进一步使用存储带有相关 B-TID 的 Ks，直到 Ks 的生存期到期，或者直到密钥 Ks 被更新。

[0779] 5.3.3 使用引导安全关联的过程

[0780] 在 UE 和 NAF 可以开始通信之前，UE 和 NAF 首先必须协商是否使用通过 GBA 方式获得的共享密钥。如果 UE 不知道与 NAF 是否使用 GBA，它使用 5.3.1 节中描述的引导初始化过程。

[0781] 一旦 UE 和 NAF 已经建立它们希望使用的 GBA，那么每次 UE 希望与 NAF 交互，则执行图 5.3 中描述的下列步骤。

[0782] 接下来，UE 和 NAF 必须协商使用哪种类型的密钥，Ks_ext_NAF 或者 Ks_int_NAF，或者以上两者。默认仅使用 Ks_ext_NAF。ME 和 NAFs 也支持这个使用，其是 GBA_U 不察觉的。如果 Ks_int_NAF，或者 Ks_ext_NAF 和 Ks_int_NAF 两者都被使用，则这个使用必须是 UE 和 NAF 间在本 5.3.3 节后面的部分中描述的过程执行之前协商好的。任何这样的协商否决 (overrule) 了密钥的默认使用。应该用在 Ua 参考点的密钥 (即 Ks_int_NAF 或 Ks_ext_NAF) 的密钥选择指示可以存在于阶段 3 规范中定义的应用专用 USS 中。如果该指示存在，NAF 应该使用指示的密钥。如果在 USS 中指示了 Ks_int_NAF 密钥，则 UE 试图使用 Ks_ext_NAF 密钥，则 NAF 应该终止与 UE 的通信。

[0783] 注意 1 :这个协商可以由定义 UE 和 NAF 之间 Ua 参考点的规范来规定，例如用于 MBMS 中 GBA 的使用的 TS 33.246，或者由 NAF 和 UE 通过 Ua 参考点协商，或者通过配置达到。

[0784] 通常，UE 和 NAF 仍将不共享保护 Ua 参考点所要求的密钥。如果它们没有这样做，则 UE 如下执行 :

[0785] - 如果需要 Ks_ext_NAF，并且 UICC 中用于选择的 UICC 应用的密钥 Ks 是有效的，则 ME 如 5.3.2 节中指定的请求 UICC 从 Ks 衍生密钥 Ks_ext_NAF。

[0786] - 如果需要 Ks_int_NAF，并且 UICC 中用于选择的 UICC 应用的密钥 Ks 是有效的，则 ME 如 5.3.2 节中指定的请求 UICC 从 Ks 衍生密钥 Ks_int_NAF。

[0787] 注意 2 :如果 UE 不希望使用相同的用于选择的 UICC 应用的 Ks 来衍生多于一个 Ks_ext/int_NAF，那么如 5.3.2 节指定的，UE 首先应该通过 Ub 参考点与 BSF 就新的密钥 Ks 达成一致，并且然后按照要求进行衍生 Ks_ext_NAF 或者 Ks_int_NAF，或者两者。

[0788] 如果用于选择的 UICC 应用的 Ks 在 UE 中不是有效的，如 5.3.2 节指定的，UE 首先通过 Ub 参考点与 BSF 就新的密钥 Ks 达成一致，并且然后按照要求进行衍生 Ks_ext_NAF 或者 Ks_int_NAF，或者两者。

[0789] 如果 NAF 与 UE 共享密钥，但是 NAF 需要这个密钥的更新，则它将向 UE 发送合适的引导重协商请求。如果密钥的生存期已经到期，则参考点 Ua 上使用的协议也将终止。这个指示的形式依靠 Ua 上参考点使用的具体的协议。如果 UE 接收到引导重协商请求，则它将如 5.3.2 节中指定的为了获得新的密钥开始 Ub 上协议的运行。

[0790] 注意 3 :如果 UE 和 NAF 之间共享的密钥成为无效，则 NAF 可以设置用于后续移除的相应安全关联的删除条件。

[0791] 注意 4 :如果 NAF 不希望使用相同 Ks 衍生多于一个的 Ks_int/ext_NAF，那么 NAF 应该总是通过将密钥更新请求发送到 UE 来回复由 UE 发送的第一请求。

[0792] 1. UE 和 NAF 现在可以按照要求，使用 Ks_ext_NAF 或者 Ks_int_NAF，或者两者通过 Ua 参考点开始与 NAF 通信。它们执行如下 :

[0793] - 如 5.3.2 节中指定的，UE 将 B-TID 提供到 NAF 以允许 NAF 从 BSF 获取相应密钥。

[0794] 注意 5 :为了允许 BSF 和 UE 中的一致密钥衍生,两者必须使用相同 FQDN 用于衍生(比较 4.5.2 节的注意 2)。对于 Ua 上使用的每个协议,如果仅 4.5.2 节的注意 2 的情况 (1) 和 (2) 被允许用于 NAF 或者如果 Ua 上使用的协议也应该通过 UE 将用于密钥衍生的 FQDN 传送到 NAF,则它应该被说明。

[0795] 注意 6 :UE 可以使 Ks_ext_NAF 或者 Ks_int_NAF 适应 Ua 参考点的特定需要。此适应处于本规范范围之外。

[0796] -ME 中 GBA 相关密钥的密钥管理 (即 Ks 和 Ks_NAF) :

[0797] - 当插入不同 UICC 时,所有 GBA 相关密钥应该从 ME 删除。因此 ME 需要在非易失性存储器中存储最新插入的 UICC 身份以能够将其与在 UICC 插入和打开电源时使用的 UICC 身份进行比较。

[0798] - 当 ME 关闭电源时,所有其他 GBA 相关密钥可从 ME 删除。如果 ME 没有在关闭电源时删除 GBA 密钥,那么 GBA 密钥需要保存在非易失性存储器中。

[0799] - 当 ME 关闭电源时,UICC 中的所有 GBA 相关密钥不需要被删除。

[0800] 注意 7 :在参考点 Ub 上每次运行了协议以后,根据 5.3.2 节,与新 B-TID 相关的新密钥 Ks 在 UE 中衍生,从而不会发生带有不同 B-TID 的密钥 Ks 同时存在于 UE 中。

[0801] - 当通过 Ub 参考点就新的密钥 Ks 达成一致并且需要衍生新的 NAF 专用的密钥用于 NAF_Id 时,那么 Ks_ext_NAF 和 Ks_int_NAF(如果存在) 应该针对此 NAF_Id 更新,但是其它相关于其它 NAF_Id 的 Ks_ext_NAF 或 Ks_int_NAF 可以存储在 UE 上。以上两种情况不应该受到影响。

[0802] 注意 8 :根据 5.3.2 节和 5.3.3 节定义的过程,UE 中存在根据 NAF_Id 存储的最多一个 Ks_int_NAF/Ks_ext_NAF 密钥对。

[0803] 注意 9 :这个规则保证了在 UE 和 NAF 处密钥 Ks_ext_NAF 和 Ks_int_NAF 总是同步的。

[0804] 2. NAF 现在通过参考点 Zn 与 BSF 开始通信。

[0805] -NAF 向 BSF 请求与 B-TID 相应的密钥,其由 UE 通过 Ua 参考点提供到 NAF。如果 NAF 是 GBA_U 不察觉的,则它通过在请求中包括标记来对齐进行指示。如果 NAF 具有几个可以与本规范中协同使用的 FQDN,那么 NAF 应该通过 Zn 在请求中发送用在 Ua 上的相同的 FQDN(见本节中以上关于密钥衍生的注意)。

[0806] -NAF 也可以请求一个或者多个与用于应用的应用专用 USS,通过 Ua 从 UE 接收的该请求可以访问。

[0807] - 通过 Zn 参考点上的密钥请求,NAF 应该向 BSF 提供 UE 已经使用以访问 NAF 的 NAF 的公共主机名,并且 BSF 应该能够验证 NAF 被授权使用这个主机名。

[0808] 3. BSF 如 5.3.2 节指定地衍生密钥 Ks_ext_NAF 和 Ks_int_NAF(如果额外需要)。如果 NAF 在它的请求中指示它是 GBA_U 察觉的,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。如果在用户 GUSS 中它们是有效的并且如果 NAF 被授权接收所请求的 USS,则 BSF 提供这些密钥的引导时间和生存期时间,以及请求的应用专用和潜在的 NAF 组专用 USS。如果由 NAF 所提供的 B-TID 所标识的密钥在 BSF 是无效的,则 BSF 应该在对 NAF 的回复中指示此情况。那么,NAF 向 UE 指示引导重协商请求。(见图 4.5)。

[0809] 注意 10 :NAF 可以根据本地策略进一步设置 Ks_NAF 的本地有效条件,例如 Ks_NAF 的重用次数的限制。

[0810] 注意 11 :NAF 以与 UE 同样的方式来使 Ks_ext_NAF 和 Ks_int_NAF,适应 Ua 参考点的特定需要。此适应处于本规范的范围之外。

[0811] -BSF 可以要求用户的 GUSS 内存在针对 NAF 的一个或多个与应用专用 USS 和潜在的 NAF 组专用 USS(见 4.4.6 节) 如果 GUSS 缺少一个或多个这些要求的设置,则 BSF 应该在向 NAF 回复中指示这一点。

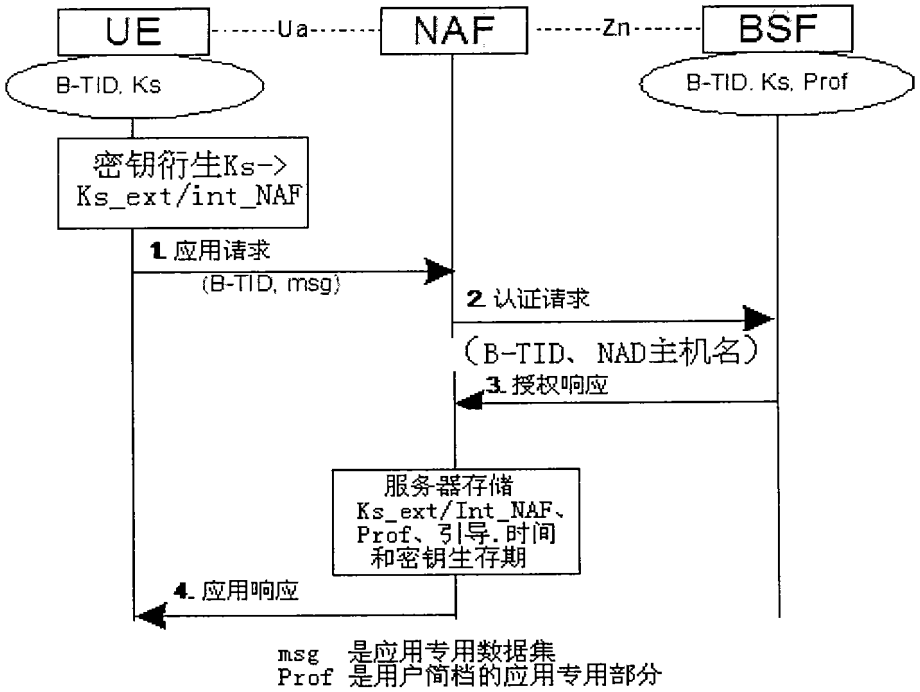
[0812] -BSF 也可以根据 BSF 的策略将私有用户身份 (IMPI) 和所请求的 USS 发送到 NAF。

[0813] 4. NAF 现在使用 Ua 参考点上使用的协议继续与 UE 交互。

[0814] - 如果 NAF 从 BSF 请求了应用专用 USS 并且该 USS 被返回到 NAF,则 NAF 应该检查此 USS 是否包含了密钥选择指示。如果存在密钥选择指示,则 NAF 应该仅使用指示的密钥。如果通过 Ua 使用不同的密钥,那么参考点 Ua 上使用的协议应该被终止。

[0815] 一旦完成了在 Ua 参考点上使用协议的运行,则由于它使 UE 和 NAF 能够以安全的方式使用 Ua 参考点,则实现了引导的目的。

[0816]



[0817] 图 5.3 :带有基于 UICC 增强的引导使用过程

[0818] 5.3.4 涉及服务发现的过程

[0819] 本文档 4.5.4 节的文本也应用于此。

[0820] 附录 A :空

[0821] 附录 B(标准化的) :

[0822] 密钥衍生函数 KDF 的规范

[0823] B.1 介绍

[0824] 本附录指定了密钥衍生函数 (KDF),其用在 GBA(即 GBA_ME) 和 GBA_U 两者中的 NAF

专用密钥衍生中。定义在本附录中的该密钥衍生函数采用下列假设：

[0825] 1. 密钥衍生函数的输入参数是八位字节字符串 - 不是任意长度的比特字符串。

[0826] 2. 单个输入参数将具有不大于 65535 个八位字节的长度。

[0827] B.2 通用密钥衍生函数

[0828] 输入参数和它们的长度应该如下连接到字符串 S 中：

[0829] 1. 八位字节中每个输入参数的长度应该编码为两个八位字节字符串：

[0830] a) 输入参数 Pi 中每个八位字节的数量表示为范围 [0,65525] 的数目 k。

[0831] b) 那么，Li 是数目 k 的两个八位字节的表示，其中 Li 的第一八位字节的最高比特等于 k 的最高比特，并且 Li 的第二八位字节的最低比特等于 k 的最低比特，

[0832] 例子：如果 Pi 包含 258 个八位字节，那么 Li 将是双八位字节字符串 0x01 0x02。

[0833] 2. 字符串 S 应该从 n 个如下的输入参数构造：

[0834] S = FC || P0 || L0 || P1 || L1 || P2 || L2 || P3 || ... || Pn || Ln

[0835] 其中

[0836] FC 是用于在算法的不同实例间区分的单个八位字节，

[0837] P0 是静态 ASCII 编码字符串，

[0838] L0 是 P0 长度的两个八位字节表示，

[0839] P1...Pn 是 n 个输入参数，并且

[0840] L1...Ln 是相应输入参数的双八位字节表示。

[0841] 3. 最终输出，即衍生的密钥等于使用密钥 Key 针对字符串 S 计算的 HMAC-SHA-256（在 [22] 和 [23] 中指定的）：

[0842] 衍生密钥 = HMAC-SHA-256(Key, S)

[0843] B.2.1 输入参数编码

[0844] 将根据 IETF RFC3629[24] 中规定的 UTF-8 编码规则来将字符串编码为八位字节串。

[0845] B.3 GBA 和 GBA_U 中 NAF 专用密钥衍生

[0846] 在 GBA 和 GBA_U 中，用于密钥衍生函数的输入参数应该如下：

[0847] -FC = 0x01，

[0848] -P1 = RAND，

[0849] -L1 = RAND 的长度是 16 个八位字节（即 0x00 0x10），

[0850] -P2 = 使用 UTF-8 编码（见 B.2.1 节）将 IMPI 编码为八位字节字符串，

[0851] -L2 = IMPI 的长度是可变的（不大于 65535），

[0852] -P3 = 使用 UTF-8 编码（见 B.2.1 节）将 NAF_ID 编码为八位字节字符串，

[0853] -L3 = NAF_ID 的长度是可变的（不大于 65535），

[0854] 第 4 章中指定的 Ks_NAF 以及第 5 章中指定的 Ks_ext_NAF 的密钥衍生中，

[0855] -P0 = “gba-me”（即 0x67 0x62 0x61 0x2d 0x6d 0x65），以及

[0856] -L0 = P0 的长度是 6 个八位字节（即，0x00 0x06）。

[0857] 在第 5 章中指定的 Ks_int_NAF 的密钥衍生中，

[0858] -P0 = “gba-u”（即 0x67 0x62 0x61 0x2d 0x2d 0x75），以及

[0859] -L0 = P0 的长度是 5 个八位字节（即，0x00 0x06）。

[0860] 用在密钥衍生中的 Key 应该是：

[0861] - 在第 4 和第 5 章中指定的 Ks（即 CK ‖ IK 连接的），

[0862] 注意：在该规范中，此函数被表示为：

[0863] Ks_NAF = KDF(Ks,“gba-me”,RAND,IMPI,NAF_Id)，

[0864] Ks_ext_NAF = KDF(Ks,“gba-me”,RAND,IMPI,NAF_Id)，

[0865] 以及

[0866] Ks_int_NAF = KDF(Ks,“gba-u”,RAND,IMPI,NAF_Id)。

[0867] 附录 C：空

[0868] 附录 D（资料性的）：

[0869] GBA 中使用的 UICC 应用用户选择的对话框实例

[0870] 对于特定情况，4.4.8 节指定用于 GBA 过程的 UICC 应用选择中的用户参与。这样包含的一个对话框窗口描述如下：

[0871] - 对话框的标题：“认证请求”。

[0872] - 解释：“服务要求你去认证，请选择你的身份：”

[0873] - 身份列表：UICC 上的可选择的应用列表。每个应用的可见文本从 UICC 上应用列表的“标签”域中摘录出来的。

[0874] - 按钮：“选择”和“取消”。

[0875] 附录 E（标准化的）：

[0876] 用于保证 Zn 的参考点安全的 TLS 简档

[0877] 保护参考点 Zn′ 安全的 TLS 简档在 RFC 3588[14]13.2 部分有详细说明。

[0878] 另外，D-Proxy 证书，即，用于 TLS 握手中使用的客户端证书应该包含 RFC 3280[17] 中指定的 subjectAltName 扩展。subjectAltName 扩展应该包含一个或者多个 dNSName 名。dNSName 名可以包含通配符‘*’以及如 RFC 2818[18]3.1 部分指定的执行匹配。

[0879] 注意：D-Proxy 证书应该包含所有 NAF 的 DNS 名，NAF 可以通过 D-Proxy 向用户的归属 BSF 发送针对 NAF 专用共享秘密的请求。如果添加了新的 NAF，则新的 DNS 名通过通配符方式（例如：″ *.operator.com″ ）被覆盖于证书中，或者需要向证书添加新的 dNSName 名。在后面的情况下，D-Proxy 需要新的证书。

[0880] 附录 F（资料性的）：

[0881] TLS 证书的处理

[0882] 对于 IPsec[19] 有效的认证框架对于 TLS 证书无效。这个附录的目的是在用于 TLS 证书的框架不存在的情况中，针对 Zn′ 参考点上的使用，提供 TLS 证书处理的指导。

[0883] 本附录中，使用下面的缩略语：CA_A 是 A 网络中的证书机构，CA_B 是 B 网络中的证书机构。$Cert_A$ 是 A 的证书，$Cert_B$ 是 B 的证书。I_A 是 A 用来识别朝向 BSF 的 NAF 的标识符集合。T_B 是 B 所信任的对等实体的集合。

[0884] F.1 TLS 证书注册

[0885] TLS 中的相互认证是基于公有密钥技术和证书达到的。TLS 对等 A 和 B 都需要包含证书存储，并且应该存在至少一个证书机构 (CA)，该 CA 可以在 A 和 B 是其一部分的安全域内发布证书。$Cert_A$ 包含 A 的标识符集合 I_A。每个标识符是全资格域名 (FQDN) 的形式。

类似的，B 的证书是 $Cert_B$。

[0886] B 存储中的证书定义 B 所信任的对等实体的组 T_B。证书的创建与注册存在几个选择，其中三个描述如下。

[0887] 1. 在第一选择中，证书机构 CA_B 仅存在于 B 的网络中。CA_B 向 B 发放证书 $Cert_B$ 并且向 A 发放证书 $Cert_A$。证书以安全方式“带外方式”从 CA_B 传送到 A 和 B。然后，A 和 B 两者都通过将对等实体证书插入证书存储中将它们的对等实体添加到它们所信任的对等实体组中：A 将 $Cert_B$ 插入到 A 的证书存储中并且 B 将 $Cert_A$ 插入到 B 的证书存储中。这个插入是典型手动的，并且细节依靠到证书存储的管理接口的实现。

[0888] 2. 在另一个选择中，A 和 B 两者的网络分别包含证书机构 CA_B 和 CA_A。CA_B 向 B 发放证书 $Cert_B$ 并且 CA_A 向 A 发放证书 $Cert_A$。证书以安全方式“带外方式”从 CA_B 传送到 A 并且从 CA_A 传送到 B。然后，A 和 B 两者都通过将对等实体证书插入证书存储中将它们的对等实体添加到它们所信任的对等实体组中：A 将 $Cert_B$ 插入到 A 的证书存储中并且 B 将 $Cert_A$ 插入到 B 的证书存储中。

[0889] 3. 在第三选择中，交换两边的 CA 证书：CA_B 的证书以安全的方式“带外方式”传送给 A 并且 CA_A 的证书以安全的方式“带外方式”传送给 B，插入到证书存储中，并且标记为可信任。TLS 握手期间换的 $Cert_A$ 和 $Cert_B$ 的确认是基于证书存储中相应 CA 证书的存在的。

[0890] 注意：在选择 1 和 2 中，如果对等实体生成自签名的证书，并且以安全的方式交换它们，则可以避免对于证书机构的需要。而且，在那些选择中可以“带外方式”交换证书指纹以代替证书本身。

[0891] F.2 TLS 证书撤销

[0892] 在 PKI- 撤消接口不存在的情况下，证书的撤消需要手动执行。撤消操作包括将 A 从 B 所信任的对等实体组 T_B 中移除。在上面描述的前两个注册选择中，通过 B 将 A 的证书 $Cert_A$ 从它的证书存储中移除进行撤销。这个移除可以手动完成。在第三选择中，A 的证书 $Cert_A$ 不在 B 的证书存储中。由于这个原因，B 必须具有通过证书的发放者检查 $Cert_A$ 的合法性的方法（同样在前两个注册选择中，如果 B 和证书发放者可以检查 $Cert_A$ 的合法性，则手动维持操作的量将减少）。这种检查可以通过使用在线证书状态协议 (OCSP) 来完成，或者通过使用由 $Cert_A$ 证书发放者公布的证书撤消列表 (CRL) 来完成。

[0893] 附录 G（标准化的）：

[0894] GBA_UUICC-ME 接口

[0895] 本附录描述了当 GBA_U 察觉的 UICC 是激活的并且 ME 被包含于 GBA 引导过程中时，UICC-ME 接口将被使用。当 UICC 应用不是 GBA_U 察觉的，如 TS 31.102[1] 和 TS 31.103[10] 中指定的，ME 在非 GBA_U 的安全上下文中使用 AUTHENTICATE 命令（即如果是 USIM 应用则使用 UMTS 安全上下文，如果是 ISIM 应用，则使用 IMS 安全上下文）。

[0896] G.I GBA_U 引导过程

[0897] 这个过程是 5.3.2 节中描述的引导过程的一部分。

[0898] ME 将 RAND 和 AUTN 发送到 UICC，其如 5.3.2 节描述的执行 Ks 衍生。

[0899] 然后，UICC 储存 Ks。UICC 也储存使用的 RAND 以识别当前引导的值。UICC 中的 RAND 值通过 ME 是可进一步可访问的。

[0900] 然后，ME 最后确定下引导过程，并且在 UICC 中存储事务标识符 (B-TID) 和与之前

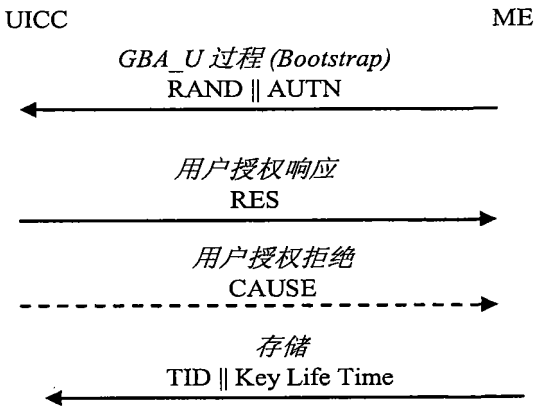
引导的密钥（即 Ks）相关的密钥生存期。UICC 中的存储事务标识符和密钥生存时间通过 ME 应该是进一步可访问的。

[0901] 在 GBA_U 引导的结尾，UICC 存储 Ks、事务标识符、密钥生存时间和 RAND。

[0902] UICC 将 RES 发送到 ME。

[0903] 新引导过程取代之前引导过程的 Ks，、B-TID、密钥生存时间和 RAND。

[0904]



[0905] 图 G.1 :GBA_U 引导过程

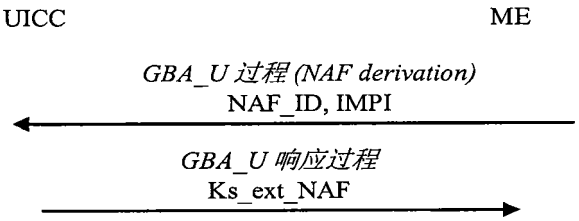
[0906] G.2 GBA_U NAF 衍生过程

[0907] 这个过程是使用 5.3.3 节描述的引导安全关联过程的一部分。

[0908] ME 将 NAF_ID 和 IMPI 发送到 UICC。然后，UICC 如 5.3.3 节描述地执行 Ks_ext_NAF 和 Ks_int_NAF 衍生。UICC 使用来自于之前引导过程存储的 RAND 和 Ks 值。UICC 返回 Ks_ext_NAF 到 ME，并且一起存储 Ks_int_NAF 和相关的 B-TID 以及 NAF_Id。

[0909] 注意 :之前需要采取之前的 GBA_U 引导。如果 UICC 中的 Ks 不是有效的，则命令将使用合适的错误信息应答。

[0910]



[0911] E.2 GBA_U_NAF 衍生过程

[0912] 附录 H（标准化的）：

[0913] Ua 安全协议标识符

[0914] H.1 定义

[0915] Ua 安全协议标示符是五个八位字节的字符串。第一八位字节表示制定 Ua 安全协议的组织。剩下的四个八位字节表示组织责任内特定的安全协议。

[0916] 对于由 3GPP 指定的所有 Ua 协议，本附录将包含这些协议的完整列表。对于由其他组织指定的所有 Ua 协议，本附录将仅指定 Ua 安全协议标识符的组织八位字节。两个组织八位字节为特殊使用而保留。

[0917] H.2 组织八位字节

[0918] 组织八位字节表示指定特别协议的组织。每个想要指定 Ua 安全协议标识符的组织应该向 3GPP 申请以接收组织八位字节值，其将在本附录中注册。下面是注册组织八位字节的列表：

[0919] “0x00”作为第一八位字节是协议没有另行指定的默认值。当八位字节“0x00”被用作第一八位字节时，仅 Ua 安全协议标识符 (0x00,0x00,0x00,0x00,0x00) 将被使用。

[0920] 注意：所有具有 Ua 安全协议标识符的协议不能彼此分开。

[0921] “0x01”.. “0xFE”作为第一八位字节表示制定 Ua 安全协议标识符的组织。

[0922] “0xFF”作为第一八位字节表示 Ua 安全协议标识符的私有范围。

[0923] 注意：具有“0xFF”作为第一八位字节的标识符可以用于定义局部 / 实验协议而不需要注册。然而，当使用这样的标识符时，可以发生攻击者可以使用 Ua 上一个安全协议中的安全漏洞在 Ua 上的不同安全协议上实施成功的攻击。

[0924] 组织的下列值被分配：

[0925] “0x01” 3GPP

[0926] 注意：具有组织八位字节“0x01”的所有协议在附录 H.3 中指定。

[0927] “0x02” 3GPP2

[0928] “0x03” 开放移动联盟

[0929] “0x04” GSMA

[0930] H.3 用于 3GPP 指定协议的 Ua 安全协议标示符

[0931] 下列 Ua 安全协议标识符由 3GPP 指定：

[0932] (0x01,0x00,0x00,0x00,0x00) 根据 TS 33.221[5] 的 Ua 安全协议。

[0933] (0x01,0x00,0x00,0x00,0x01) 根据 TS 33.246[26] 的 Ua 安全协议。注意：TS 33.246[26] 提供 HTTP 摘要和 MIKEY 协议中使用的密钥间的密钥分离。

[0934] (0x01,0x00,0x00,0x00,0x02) 根据 TS 24.109[29] 的 Ua 安全协议 HTTP 摘要认证，除非 HTTP 摘要认证被用在另一个 Ua 安全协议的上下文中，其已经在本附录中的其他地方被覆盖。

[0935] (0x01,0x00,0x01,yy,zz) 根据 TS 33.222[25] 用于“使用基于证书的 NAF 认证的共享基于密钥的 UE 认证”的 Ua 安全协议，或者根据 TS 33.222[25] 的用于“UE 和 NAF 间的共享基于密钥德相互认证”的 Ua 安全协议。这里，“yy，zz”是根据针对 TLS V 1.0 中 TLS Ciphersuites 定义的值以及针对 TLS[27] 的 PSK Ciphersuite 的保护机制 Ciphersuite 代码。

[0936] 注意：例子：RFC2246[28]CiphersuiteTLS_RSA_WITH_3DES_EDE_CBC_SHA 具有代码＝ {0x00,0x0A}，因此相应协议标识符应该是 (0x01,0x00,0x01,0x00,0x0A)。

[0937] 附录 I（标准化的）：

[0938] 2G GBA

[0939] 本附录指定实现选项以允许用于 GBA 的 UICC 上的 SIM 卡或者 SIM 的使用。本附录中指定的过程被称作 2G GBA。2G GBA 允许以比使用口令或者使用无增强的 GSM 更安全的的方式访问应用。它对于仍旧没有全面部署 USIM 的运营商是有用的。

[0940] I.1 参考模型

[0941] 参考模型与 4.1 节中描述的相同。

[0942] I.2 网元

[0943] I.2.1 引导服务器功能 (BSF)

[0944] 通用引导服务器功能 (BSF) 和 UE 将使用 2G AKA 协议和 TLS 协议相互认证，并且就向后应用于 UE 和网络应用功能 (NAF) 之间的会话密钥达成一致。BSF 将通过使用附录 B 中执行的密钥衍生过程限制密钥资料到特定 NAF 的适用性。密钥衍生过程可以在密钥资料的生存期与多个 NAF 使用。密钥资料的生存期根据 BSF 的本地策略被设置。密钥资料的生成在 I.5.2 节中指定。

[0945] BSF 将能够从 HSS 获取 GBA 用户安全设置 (GUSS)。

[0946] BSF 将能够从由 HSS 发送的认证向量的类型发现用户是 2G 用户还是 3G 用户。

[0947] BSF 应该能够保留列表，其分配 NAF 到 NAF 组。这个列表用来选择在 GUSS 中哪一个应用专用的 USS 以及是否有应用专用的 USS 对于特定 NAF 是有效的。

[0948] 注意 1：运营商分配 NAF 到 NAF 组。HSS 中的 NAF 组定义以及所有连接的属于相同运营商网络的 BSF 都应该是相等的。由于这些网元属于相同运营商网络，所以在 3GPP 中不必对 NAF 组定义自身进行标准化。

[0949] 注意 2：NAF 分组可以是例如“归属”和“拜访”。它允许 BSF 例如在归属网络或拜访网络中发送 USS 用于具有例如不同授权标记的相同应用到不同的 NAF。例如在拜访网络中，NAF 仅指示请求的应用，但是不会察觉用户的归属网络中的分组。

[0950] I.2.2 网络应用功能 (NAF)

[0951] 已经完成引导之后，UE 和 NAF 可以运行一些应用专用协议，其中消息的认证将基于 UE 和 BSF 间相互认证期间生成的那些会话密钥。

[0952] 对于 NAF 功能性的通常假设：

[0953] - 在 UE 和 NAF 之间不需要存在预先的安全关联；

[0954] -NAF 应该能够定位并且与用户的 BSF 进行安全的通信。

[0955] - 在应用专用协议的运行期间，NAF 能够获得 UE 和 BSF 之间建立的共享密钥资料。

[0956] -NAF 能够通过 BSF 从 HSS 获得零个或多个应用专用的 USS；

[0957] -NAF 能够根据本地策略设定共享密钥资料的本地有效条件。

[0958] -NAF 能够检查共享密钥资料的生存期和本地有效条件。

[0959] -NAF 能够具有是否接受 2G 用户的策略。

[0960] 注意：没有额外测量的情况下，GBA 不保证密钥的刷新，某种意义上，Ks(int/ext) NAF 不保证密钥没有被用于 Ua 协议的之前运行中。UE 和 NAF 可以采取的以保证 GBA 中的密钥刷新的额外的方法是：

[0961] 1) 在衍生新 Ks_NAF 之前，强制 Ub 协议的新运行（从而产生新 Ks)。

[0962] 2) 存储以前使用的密钥 Ks(_int/ext)_NAF，或者相应的密钥标识符 B-TID，直到它们生存期结束。

[0963] 支持 Ua 协议（其在协议的无连接运行上不提供回放保护）的 UE 和 NAF 在需要的时候将需要采取相应行动以避免回放攻击。

[0964] I.2.2a 直径协议 (D 代理）

[0965] 来自于 4.2.2a 节的文本也应用于此。

[0966] 1.2.3 HSS

[0967] 所有用户安全设置的集合 (USS)，即 GUSS，存储在 HSS 中。

[0968] HSS 的要求是 ：

[0969] -HSS 应该仅对于 GUSS 提供永久性存储 ；

[0970] -GUSS 应该以这样的方式定义，即对于标准化应用简档不同运营商的交互是可能的。

[0971] -GUSS 应该以这样的方式定义，即不需要这些元素的标准化而支持运营商指定应用和对于现存应用简档的扩展。

[0972] -GUSS 应该能够包含应用专用 USS，该 USS 包含 GBA_U 情况中的密钥选择指示 (即，是否 NAF 应该使用 Ks_ext_NAF 或者 Ks_int_NAF)、由一个或者多个 NAF 主持的一个或多个应用的标识或者鉴权信息的相关参数。任何其他类型的参数在应用专用 USS 中不允许。

[0973] 注意 1 ：可以由 NAF 直接从 HSS 获取必要的用户简档数据，或可以利用应用专用 USS 提供的身份信息从其本地数据库获取。

[0974] 注意 2 ：如果临时从用户撤销服务，则 HSS 可以从 GUSS 中临时移除这个应用专用 USS。

[0975] -GUSS 应该能够包含针对 BSF 使用的参数 ：

[0976] - 用户特定的密钥生存期。

[0977] - 可选择的，时间戳指示 GUSS 已经由 HSS 最后修改的时间。

[0978] 注意 3 ：这些参数是可选的，如果用户的 GUSS 缺少它们或者用户没有 GUSS，那么 BSF 将使用由特别 MNO 定义的 BSF 本地策略中的缺省值。

[0979] HSS 应该能够分配应用专用 USS 到 NAF 组。这将以这样的方式定义，即对于相同应用，但是不同 NAF 组的不同 USS 是可能的。每 GUSS 的 USS 的数量限制依赖于通过运营商的 NAF 分组使用。

[0980] - 如果没有针对这个应用定义 NAF 组，那么每个应用最多有一个 USS 存储在 GUSS 中。

[0981] - 如果针对这个应用定义了 NAF 组，那么每个应用最多有一个 USS 和 NAF 组存储在 GUSS 中。

[0982] -HSS 中的 NAF 组定义和所有连接的属于相同运营商网络的 BSF 应该是相等的。

[0983] - 对于 2G 用户而言，关于 UICC 类型和密钥选择的信息是不要求的。

[0984] 2G GBA 被认作基于 ME。

[0985] I.2.4 UE

[0986] 从 UE 要求的功能性是 ：

[0987] - 支持 HTTP 摘要 AKA 协议 ；

[0988] - 支持 TLS ；

[0989] - 在引导中使用 SIM 的能力 ；

[0990] - 对于 ME 上的 Ua 应用，向 ME 上的 GBA 功能指示是否 SIM 被允许用在引导中的能力 (见 I.4.8 节) ；

[0991] - 从 Kc、RAND、SRES 和 Ks- 输入衍生将和 Ua 接口上的协议一起使用的新密钥资料的能力 ；

[0992] - 支持 NAF 应用专用协议 (例子见 TS 33.221[5])。

[0993] 2G GBA 察觉的 ME 应该支持如 5.2 节中指定的 3G GBA_U 和如 4.5 节中指定的 3G GBA_ME 两者。

[0994] I.3 引导架构和参考点

[0995] I.3.1 参考点 Ub

[0996] 参考点 Ub 处于 UE 和 BSF 之间。参考点 Ub 提供 UE 和 BSF 间的相互认证。它允许 UE 基于 2G AKA 基础结构引导会话密钥。

[0997] I.3.2 参考点 Ua

[0998] 参考点 Ua 承载应用协议，使用作为参考点 Ub 上协议运行的结果的 UE 与 BSF 之间协商的密钥资料保证其安全。

[0999] I.3.3 参考点 Zh

[1000] 使用于 BSF 和 HSS 之间使用的参考点 Zh 允许 BSF 从 HSS 获得必要的认证信息和所有的 GBA 用户安全设置。到 2G 认证中心的接口是 HSS 内部的，并且不需要作为此架构的一部分进行标准化。

[1001] I.3.4 参考点 Zn

[1002] 参考点 Zn 由 NAF 使用以获取之前协议从 UE 到 BSF 在参考点 Ub 上运行期间协商的密钥资料。如果 NAF 请求，它也被用于从 BSF 获取应用专用的用户安全设置。

[1003] I.4 引导的要求和原理

[1004] 下面的要求与原理可应用于引导过程：

[1005] - 引导功不依赖特定的 NAF；

[1006] - 实现引导功能的服务器需要被本地运营商所信任以处理认证向量；

[1007] - 实现 NAF 的服务器需要被本地运营商所信任以处理衍生的密钥资料；

[1008] - 可以在运营商的本地网络和拜访网络中支持 NAF；

[1009] - 该架构不排除在第三网络中对网络应用功能的支持；

[1010] - 在可能的程度上，应该重新利用现存协议和基础设施；

[1011] - 为了确保宽广的适用性，所有相关协议优选运行于 IP 上；

[1012] - 应该阻止正在使用 GBA 的一个 NAF 中的安全漏洞被攻击者用来对使用 GBA 的其它 NAF 实施成功的攻击。

[1013] -UICC 上的现存 SIM 卡以及它们的规范不应该被影响。

[1014] - 如果 USIM 和 ISIM 是有效的，则它们应该如第 4 和 5 章中指定的适用，并且不应该使用 2G GBA。

[1015] -2G GBA 不应该影响如第 4 和 5 章中指定的基于 USIM/ISIM 的 GBA。

[1016] -2G GBA 不应该减少 USIM/ISIM 用户的安全性。

[1017] -2G GBA 应该最小化对于第 4 章中指定的基于 USIM/ISIM 的 GBA 的改变。

[1018] -2G GBA 应该提供方法以减轻 GSM 的已知弱点。

[1019] I.4.1 接入独立性

[1020] 引导过程是接入独立的。引导过程需要来自于 UE 的 IP 连接。

[1021] I.4.2 认证方法

[1022] 在没有有效的蜂窝订阅的情况下，UE 与 BSF 之间的认证应该是不可能的。认证应该基于 GSM 认证（也称作 2G AKA）协议。另外，BSF 认证应该是附加地基于带有服务器证

书的 TLS。

[1023] I].4.3 漫游

[1024] 来自于 4.4.3 节的文本也应用于此。

[1025] I.4.4 参考点 Ub 的要求

[1026] 参考点 Ub 的要求是 :

[1027] -BSF 应该能够识别 UE ;

[1028] -BSF 和 UE 应该能够基于 I.4.2 中的方法彼此认证 ;

[1029] -BSF 应该能够发送引导事务标识符到 UE ;

[1030] -UE 和 BSF 应该建立共享密钥 ;

[1031] -BSF 应该能够向 UE 指示密钥资料的生存期。由 BSF 通过 Ub 发送的密钥生存期将指示密钥的到期时间。

[1032] 注意 :这并未排除 UE 根据 UE 的本地策略在到期时间之前刷新密钥。

[1033] I.4.5 参考点 Zh 的要求

[1034] 参考点 Zh 的要求是 :

[1035] - 应该提供相互认证、保密性和完整性 ;

[1036] 注意 1 :如果 BSF 和 HSS 位于相同运营商网络内,此要求可以通过物理的或者专有的安全方式来满足。

[1037] -BSF 应该能够发送关于用户的引导信息请求 ;

[1038] - 可选择地,BSF 可以具有能够将用户的 GBA 用户安全设置的时间戳发送到 HSS(时间戳选项) 的能力 ;

[1039] -HSS 应该能够发送 2GP AKA 向量到 BSF ;

[1040] -HSS 应该能够为了安全目的的需要将用户的 GBA 用户安全设置的完整集合发送到 BSF ;可选择地,HSS 可以具有向 BSF 指示 BSF 是否已经基于 GUSS 时间戳 (时间戳选项) 具有 GUSS 的最新副本的能力。

[1041] 注意 2 :如果用户的 GUSS 在 HSS 中进行了更新,则此消息不传送至 BSF。作为引导过程的一部分,当 BSF 下次通过 Zh 参考点从 HSS 获取认证向量和 GUSS 的时候,BSF 中的 GUSS 会被更新。

[1042] - 在 HSS 中不需要关于引导的状态信息 ;

[1043] - 参考点 Zh 上的所有过程应该由 BSF 初始化的 ;

[1044] - 到 HSS 的不同接口的数量应该最少。

[1045] I.4.6 参考点 Zn 的要求

[1046] 参考点 Zn 的要求是 :

[1047] - 应该提供相互认证、保密性和完整性 ;

[1048] - 如果 BSF 和 NAF 位于相同的运营商的网络内,则 Zn 参考点应该根据 NDS/IP[13] 受到保护 ;

[1049] - 如果 BSF 和 NAF 位于不同的运营商的网络中,则在 D-Proxy 和 BSF 之间的 Zn' 参考点应该使用如 RFC 2246[6] 中指定的 TLS 来保证安全 ;

[1050] 注意 1 :附录 E 指定用于保证 Zn' 参考点的安全的 TLS 简档。

[1051] -BSF 应该验证请求 NAF 被授权以获得密钥资料或者密钥资料和请求的 USS ;

[1052] -NAF 应该能够发送密钥资料请求到 BSF，包含由 UE 的相应请求使用的 NAF 的公共主机名。BSF 应该能够验证 NAF 被授权以使用此主机名，即，当它联系 NAF 时，由 UE 使用 FQDN；

[1053] -BSF 应该能够发送密钥资料到 NAF；

[1054] -NAF 应该能够从 BSF 获得应用专用 USS 选择的集合，根据 BSF 的策略以及来自于 Zn 上的 NAF 的请求中指示的应用；

[1055] -NAF 应该能够向 BSF 指示需要 USS 的单个应用或几个应用；

[1056] 注意 2：如果一些应用只需要应用专用的 USS 的子集，则 NAF 从发送自 BSF 的完整 USS 集合中选择这个子集。

[1057] - 如果私有用户身份和应用专用的 USS 可以被发送至 NAF，则 BSF 应该能够在每个 NAF 或每个应用基础之上配置；

[1058] - 如果 NAF 从 BSF 请求 USS 并且它们没有出现在用户的 GUSS 中，它不应引起错误，假设满足 BSF 本地策略的条件。然后，BSF 应该仅将请求的和发现的 USS 发送到 NAF；

[1059] - 如下配置本地策略是可能的：BSF 可以要求一个或者多个应用专用的 USS 存在于用于特定的请求 NAF 的特定用户的 GUSS 中，并且如果不满足条件，则拒绝来自于 NAF 的请求。为了满足这个本地策略，NAF 不需要通过 Zn 参考点请求 USS，BSF 要求其存在于 GUSS 中，更确切地说 BSF 检查 USS 的本地存在已经足够了。以没有 USS 被要求用于请求 NAF 这样的方式配置 BSF 也应该可能的；

[1060] -BSF 应该能够向 NAF 指示引导的时间和密钥资料的生存期。由 BSF 通过 Zn 发送的密钥生存期应该指示密钥的到期时间，并且应该与由 BSF 通过 Ub 发送到 UE 的密钥的生存期一致。

[1061] 注意 3：这不能排除 NAF 根据 NAF 的本地策略在到期时间之前刷新密钥。

[1062] 注意 4：如果一个或者多个已经发送到 NAF 的 USS 已经在 HSS 中的用户 GUSS 中更新了，则此变化在下次它通过 Zn 参考点从 BSF 获取 USS 时传送至 NAF（假设 BSF 已经通过 Zh 参考点从 HSS 更新了用户的 GUSS）。

[1063] -BSF 应该将信息发送到 NAF 表明用户是 2G 用户。如果没有这样的信息被发送，则 NAF 将假设用户是 3G 用户。

[1064] 注意 5：此要求使 NAF 能够根据它的本地策略接受 2G 用户。第二句保证了与本规范的第 4 和 5 章中指定的过程向后兼容。还要注意在 GUSS 中包含有关用户类型的信息将不足以满足此要求，因为 GUSS 不为每个用户而存在。

[1065] -BSF 可以根据它的本地策略确定 NAF 将不服务于 2G 用户。如果是这样的情况，BSF 不发送密钥到 NAF。

[1066] 注意 6：此要求允许控制 BSF 的运营商确定哪个应用将仅使用 3G 安全。此要求对于 NAF 也是必需的，其不能够评估关于由 BSF 发送的订阅类型的信息，例如，预发布 7NAF。

[1067] I.4.7 引导事物标示符的要求

[1068] 引导事务标识符 (B-TID) 应该用于将用户身份绑定到参考点 Ua，Ub 和 Zn 中的密钥资料。

[1069] B-TID 的要求是：

[1070] -B-TID 应该是全局唯一的；

[1071] -B-TID 应该是可用为用在参考点 Ua 上的协议中的密钥标识符；

[1072] -NAF 应该能够从 B-TID 中检测 UE 的归属网络和 BSF。

[1073] 注意 1：密钥已经无效之后，NAF 可以基于删除条件移除安全关联。

[1074] 注意 2：不得不注意 UE 和 NAF 之间的 GBA 和非 GBA 认证的并行使用不导致冲突，例如，在命名空间中。这种潜在的冲突不能以通用的方式解决，因为它依靠于 UE 和应用服务器之间使用的专用协议和认证机制。因此，它处于本规范的范围之外。

[1075] 对于 UE 和 NAF 之间使用的 HTTP 摘要认证的例子，如下应用的并行使用是可能的：<用户名，密码>对对于仅一个域必须是唯一的。由于 NAF 控制域名，则它必须确保只有基于 GBA 的域才能以保留的 3GPP 域名命名。在 NAF 希望允许基于非 GBA 的认证也处于 GBA 域中的特殊的情况下，它必须确保没有 B-TID 格式的用户名被用在基于 GBA 的认证之外。

[1076] I.4.8 UICC 应用的选择和 SIM 卡的要求

[1077] 如果 UE 中存在 UICC，包含 USIM 或 ISIM，那么 USIM 或 ISIM 将如 4.4.8 节中指定的被使用。否则将使用 SIM。

[1078] 如果没有 UICC，但是 UE 中存在 SIM 卡，则将使用 SIM 卡。

[1079] I.4.9 参考点 Ua 的要求

[1080] 来自于 4.4.9 节的文本也应用于此。

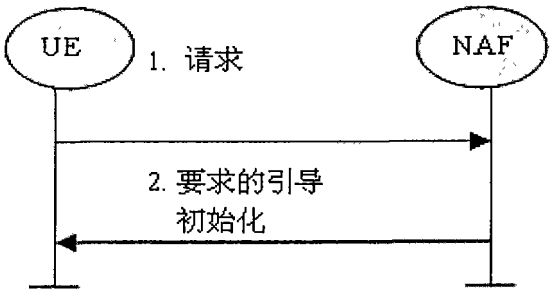
[1081] I.5 过程

[1082] 本章详细指定由不同应用进一步利用的 2G GBA 引导过程的格式。它包含使用 BSF 的认证过程，以及密钥资料生成过程。

[1083] I.5.1 引导的初始化

[1084] 在 UE 和 NAF 间的通信可以开始之前，UE 和 NAF 首先必须协商是否使用 GBA。当如果 UE 希望与 NAF 交互时，但是它不知道 NAF 是否需要使用通过 GBA 方式获得的共享密钥，这时，UE 将联系 NAF 以获得进一步的指示（见图 I.2）。

[1085]



[1086] 图 I.2：引导的初始化

[1087] 1. UE 通过参考点 Ua 发起与 NAF 的通信而没有任何 GBA 相关参数。

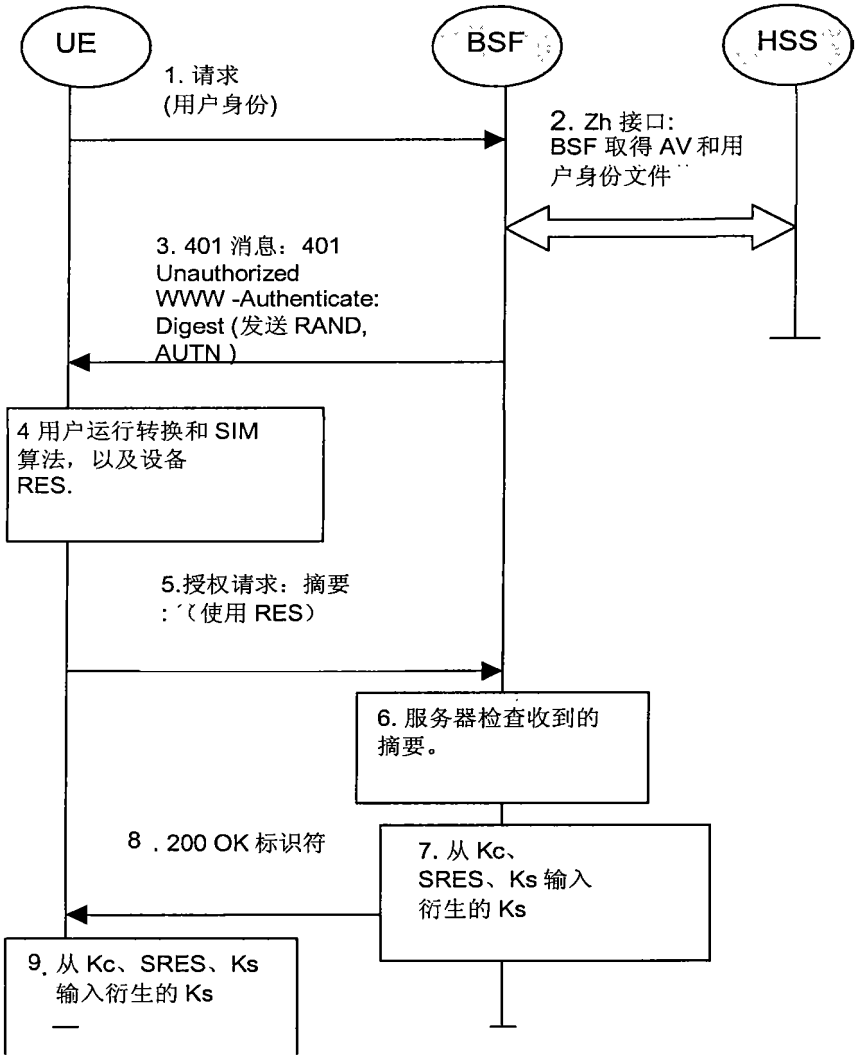
[1088] 2. 如果 NAF 需要使用通过 GBA 获得的共享密钥，但是来自 UE 的请求中不包括 GBA 相关参数，则 NAF 使用引导初始化消息进行回复。这种指示方式可以依靠于特定的参考点 Ua 并且在相关的阶段 3 规范中指定。

[1089] I.5.2 引导过程

[1090] 当 UE 希望与 NAF 交互，并且它知道需要引导过程时，那么它将首先执行引导认证（见图 I.3）。否则，仅当它已经接收引导初始化要求消息或者来自 NAF 的引导协商指示时，

或者当 UE 中的密钥生存期已经到期时，UE 应该执行引导认证。（协议 I.5.3 子节）。

[1091]



[1092] 图 I.3 引导过程

[1093] 1. UE 与 BSF 建立保密保护的 TLS 隧道。在 TLS 隧道建立中，UE 应该通过 BSF 提供的证书来认证 BSF。UE 应该检查包含存在于 BSF 提供的证书中的 BSF 的相同 FQDN 的“域”属性。所有 ME 和 BSF 间的进一步通信通过此 TLS 隧道发送。UE 现在发送初始 HTTPS 请求。

[1094] 2. BSF 通过 Zh 从 HSS 请求认证向量和 GUSS。HSS 通过 Zh 参考点返回 GBA 用户的安全设置 (GUSS) 的完整集合和一个 2G 认证向量 (AV = RAND，SRES，Kc)。BSF 通过观察认证向量类型发现 UE 配备有 2G SIM。

[1095] 如果 BSF 实现时间戳选项并且具有在以前引导过程期间从 HSS 已经获得的用户的 GUSS 的本地副本，并且此 GUSS 包括时间戳，则 BSF 可以在请求消息中包括 GUSS 时间戳。当接收那个时间戳时，如果 HSS 实现了时间戳选项，则 HSS 可以将其与存储在 HSS 中的 GUSS 时间戳进行比较。在此情况中，如果并且仅如果 HSS 已经完成比较并且时间戳是相等的，那么 HSS 应该发送“GUSS 时间戳相等”指示到 BSF。在任何其他情况中，HSS 应该发送 GUSS（如果有效）到 BSF。如果 BSF 接收到“GUSS 时间戳相等”的指示，它将保留 GUSS 的本地副本。

在任何其他情况中，BSF 应该删除 GUSS 的本地副本，并且存储接收的 GUSS（如果发送了）。

[1096] BSF 将一个 2G 认证向量 (RAND，SRES，Kc) 转换到参数 RES。

[1097] -RES = KDF(key，“3gpp-gba-res”，SRES)，截取 128 比特，其中 key = Kc ‖ Kc ‖ RAND 并且 KDF 是 TS 33.220 的附录 B 中指定的密钥衍生函数。

[1098] BSF 也应该选择 128 比特随机数“Ks- 输入”并且在 HTTP 摘要 AKA 的 aka-nonce 中设置服务器专用数据 = Ks- 输入，参考 [4]。

[1099] 注意“截取 128 比特”意味着从 KDF 的 256 比特输出中，使用编号为 [0] 到 [127] 的 128 比特。

[1100] 3.BSF 将在 401 消息中将 RAND 和服务器专用数据转发到 UE（没有 RES）。这是要求 UE 认证自己。BSF 应该在 www- 认证头中设置 qop = int（比较 [3]）。

[1101] 4.UE 从消息中抽取 RAND 并且计算相应 Kc 和 SRES 值。然后，它如步骤 2 中指定的从这些值计算参数 RES。

[1102] 5.UE 发送另一个包含摘要 AKA 响应（使用 RES 作为口令来计算）和 cnonce（参考 [3]）的 HTTP 请求到 BSF。

[1103] 6.BSF 通过验证摘要 AKA 响应来对 UE 进行认证。如果认证失败，则 BSF 将不在任何进一步的通信中重用认证向量。

[1104] 7.BSF 通过计算 Ks = KDF(key，Ks- 输入，“3gpp-gba-res”，SRES) 生成密钥资料 Ks。通过采用来自于步骤 3 的 base64 编码的 [12]RAND 值和 BSF 服务器名，即 base64encode(RAND)@BSF_servers_domain_name 以 NAI 的格式生成 B-TID 值。

[1105] 8.BSF 应付发送包括 B-TID 和 authentication-info 头（参考 [3]）的 200 OK 消息到 UE 以指示认证成功。另外，在这个 200 OK 消息中，BSF 应该提供密钥 Ks 的生存期。

[1106] 9. 如果根据 [3] 服务器认证失败，则 UE 应该放弃过程。如果成功了，则 UE 应该以与 BSF 相同的方式生成密钥资料 Ks。

[1107] 10.UE 和 BSF 两者都应该使用 Ks 以衍生密钥资料 Ks_NAF，从而与如 I.5.3 节中指定的过程一起使用。Ks_NAF 应该用于保证参考点 Ua 的安全。

[1108] 以 Ks_NAF = KDF(Ks，″ gba-me″，RAND，IMPI，NAF_Id) 计算 Ks_NAF，其中 KDF 是附录 B 中指定的密钥衍生函数，并且密钥衍生参数包括用户的 IMPI，NAF_Id 和 RAND。NAF_Id 包括 NAF 的全 DNS 名，与附录 H 中指定的 Ua 安全协议标识符连接。KDF 应该在 ME 中实现。

[1109] 注意 3：为了允许基于 UE 和 BSF 中 NAF 名称的一致密钥衍生，应满足下列三个前提条件中的至少一个：

[1110] (1) 在 DNS 中，已知 NAF 仅在一个域名下 (FQDN)，即，没有两个不同域名指向 NAF 的 IP 地址。这必须通过管理装置完成。

[1111] (2)NAF 的每个 DNS 入口指向不同的 IP 地址。NAF 响应所有这些 IP 地址。每个 IP 地址通过 NAF 配置绑定到相应的 FQDN。NAF 可以从 IP 地址看到哪个 FQDN 用于密钥衍生。

[1112] (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，以在适当的时候在与 UE 的所有通信中使用这个名字，并且将这个名字传送给 BSF 以允许 Ks_NAF 的正确衍生。

[1113] 在 Ua 上 TLS 隧道的情况下，这需要用于 NAF 的多身份证书或 Ua 上的 RFC 3546[9]

或者 Ua 上带有类似目的的其他的协议方法的部署。

[1114] UE 和 BSF 应该存储带有相关 B-TID 的密钥 Ks 用于将来的使用，直到 Ks 的生存期已经到期，或者直到密钥 Ks 被更新。

[1115] I.5.3 使用引导安全关联的过程

[1116] 在 UE 和 NAF 可以开始通信之前，UE 和 NAF 首先必须协商是否使用通过 GBA 获得的共享密钥。如果 UE 不知道与 NAF 是否使用 GBA，它使用 I.5.1 节中描述的引导初始化过程。

[1117] 一旦 UE 和 NAF 已经建立它们希望使用的 GBA，那么每次 UE 希望与 NAF 交互，则执行图 I.4 中描述的下列步骤。

[1118] 1.UE 通过参考点 Ua 与 NAF 开始通信：

[1119] -通常，UE 和 NAF 将不共享保护参考点 Ua 所要求的密码。如果它们已经共享了该密钥（即，如果用于相应的密钥衍生参数 NAF_Id 密钥 Ks_NAF 已经是有效的），则 UE 和 NAF 就可以立刻开始安全的通信。如果 UE 和 NAF 还没有共享密钥，则 UE 如下继续执行：

[1120] -如果 UE 中用于选择的 UICC 应用的密钥 Ks 是有效的，则如 I.5.2 节制定的 UE 从 Ks 衍生密钥 Ks_NAF；

[1121] -如果 UE 中没有用于选择的 UICC 应用的密钥 Ks 是有效的，则 UE 首先通过参考点 Ub 与 BSF 协商新密钥 Ks，并且然后进行衍生 Ks_NAF 的过程；

[1122] 注意 1：对于，如果 UE 不希望使用用于 UICC 应用的相同 Ks 密钥衍生多于一个 Ks_NAF，那么 UE 就应该首先通过参考点 Ub 与 BSF 协商新的密钥 Ks，然后进行衍生 Ks_NAF 的过程。

[1123] -如果 NAF 与 UE 共享密钥，但是 NAF 要其更新该密钥，例如，因为密钥的生存期已经到期或者很快将到期，或者该密钥不能满足 NAF 本地有效条件，则它应该发送合适的引导的重协商请求到 UE，见图 I.5。如果密钥的生存期已经到期，则通过参考点 Ua 使用的协议将被终止。这个指示的形式依靠参考点 Ua 上使用的特定协议。如果 UE 接收了引导重认证请求，则它为了获得新密钥 Ks，如 I.5.2 节指定的，开始参考点 Ub 上协议的的运行。

[1124] 注意 2：为了允许 UE 和 BSF 中的一致密钥衍生，两者都必须使用相同的 FQDN 进行衍生（见 I.5.2 节的注意 2）。如果只有 I.5.2 节的注意 1 的 (1) 和 (2) 被允许用于 NAF，或者如果 Ua 上使用的协议也将通过 UE 到 NAF 传输用于密钥衍生的 FQDN，则对于每个使用在 Ua 上的协议，它将被指定。

[1125] 注意 3：如果 UE 和 NAF 之间的共享密钥是无效的，则 NAF 就可以为后续删除设置相应安全关联的删除条件。

[1126] -UE 以 I.3.2 节中指定的格式向 NAF 提供 B-TID，以允许 NAF 从 BSF 获取相应的密钥。

[1127] 注意 4：UE 可以使密钥资料 Ks NAF 适应于参考点 Ua 的特定需要。此适应在本规范的范围之外。

[1128] -ME 中 GBA 相关密钥的密钥管理（即 Ks 和 Ks_NAF）：

[1129] -当插入不同 UICC 或 SIM 卡时，所有 GBA 相关密钥应该从 ME 删除。因此 ME 需要在非易失性存储器中存储最新插入的 UICC 身份或 SIM 卡身份以能够将其与在 UICC 插入和打开电源时使用的 UICC 身份或 SIM 卡身份进行比较。

[1130] -ME 关闭电源时，密钥 Ks 应该从 ME 删除。

[1131] -ME 关闭电源时，所有其他 GBA 相关密钥可从 ME 删除。如果 ME 没有在关闭电源时删除 GBA 密钥，那么 GBA 密钥需要保存在非易失性存储器中。

[1132] - 当通过参考点 Ub 协商出新 Ks 并且衍生于一个 NAF_Id 的密钥 Ks_NAF 被更新时，衍生于不同 NAF_Id 的存储在 UE 上的其他 Ks_NAF 将不会受到影响。

[1133] 注意 5：根据 I.5.2 节和 I.5.3 节中定义的过程，在 UE 中针对每个 NAF-Id 最多存储一个 Ks_NAF。

[1134] 2. NAF 通过参考点 Zn 与 BSF 开始通信，

[1135] -NAF 请求对应于由 UE 通过参考点 Ua 提供给 NAF 的 B-TID 的密钥资料。如果 NAF 具有几个可以与本规范联合使用的 FQDN，那么 NAF 应该通过 Zn 在请求中传输用在 Ua 上的相同 FQDN（见本节中关于密钥衍生的注意 2）；

[1136] -UE 也可以请求一个或者多个应用专用 USS 用于应用，其通过 Ua 从 UE 接收的请求可以访问；

[1137] - 通过密钥资料请求，NAF 应该提供 UE 已经使用去访问 NAF 的主机名到 BSF，并且 BSF 应能够验证该 NAF 被授权使用该主机名。

[1138] 3. BSF 从密钥 Ks 和密钥衍生参数衍生保护参考点 Ua 上使用的协议所要求的密钥，如 I.5.2 节中指定的，并且如果在用户 GUSS 中它们是有效的并且如果 NAF 被授权接收所请求的 USS，则向 NAF 提供被请求的密钥 Ks_NAF 以及引导时间和密钥的生存期，以及请求的应用专用和潜在的 NAF 组专用 USS。另外，BSF 应该向 NAF 指示用户是 2G 用户。如果由 NAF 所提供的 B-TID 所标识的密钥在 BSF 是无效的，则 BSF 将在对 NAF 的回复中对此进行指示。那么，NAF 向 UE 指示引导重协商请求。

[1139] 注意 6：NAF 可以根据本地策略，进一步设置 Ks_NAF 的本地有效条件。例如 Ks_NAF 重用次数限制。

[1140] 注意 7：NAF 将使用与 UE 同样的方式使 Ks_NAF 适应参考点 Ua 的指定要求。该适应在本规范的范围之外。

[1141] -BSF 可以要求在用户的 GUSS 内存在用于 NAF 的一个或多个应用专用 USS 以及潜在的 NAF 组专用 USS（见 I.4.6 节）。如果 GUSS 缺少一个或多个这些要求的设置，则 BSF 将在对 NAF 的回复中指示这一点。

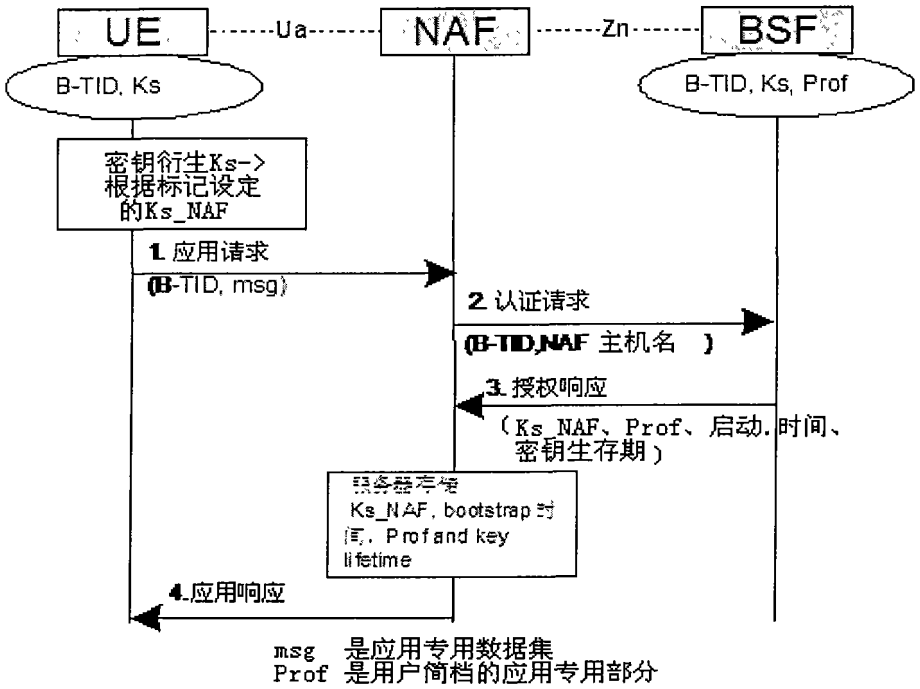
[1142] -BSF 还可能根据 BSF 的策略将私有用户标识（IMPI）和所请求的 USS 发送给 NAF。

[1143] - 如果 BSF 或者 NAF 根据它们的本地策略确定 NAF 不服务于 2G 用户，则 NAF 应该终止参考点 Ua 上的协议。

[1144] 4. NAF 通过参考点 Ua 上使用的协议继续与 UE 交互。

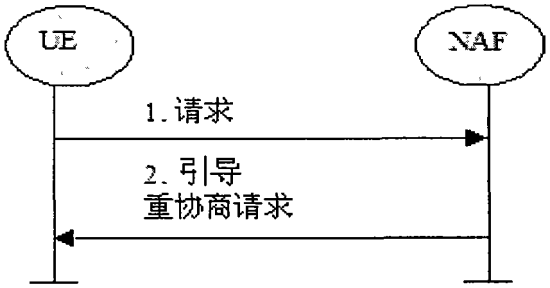
[1145] 一旦在参考点 Ua 上使用协议的运行完成，则达到了引导的目的，因为它使 UE 和 NAF 能够以安全的方式使用参考点 Ua。

[1146]



[1147] 图 I.4 引导使用过程

[1148]



[1149] 图 I.5 :引导重协商请求

[1150] I.5.4 涉及服务发现的过程

[1151] UE 将从 SIM 上的 IMSI 发现 BSF 的地址。将使用 4.5.4 节中指定的相同的发现过程。

[1152] I.6 TLS 简档

[1153] UE 和 NAF 将支持 RFC 2246[6] 和 WAP-219-TLS[30] 中指定的 TLS 版本或者更高的版本。

[1154] 注意 1 :根证书的管理处于此技术规范的范围之外。

[1155] 注意 2 :证书的撤消处于此技术规范的范围之外。然而,如果 BSF 证书可以折中,应该注意对于 BSF 证书选择短的生存期可以显著减少风险。

[1156] I.6.1 保护机制

[1157] UE 应该使用 CipherSuite TLS_RSA_WITH_3DES_EDE_CBC_SHA 或 CipherSuiteTLS_RSA_WITH_AES_128_CBC_SHA。

[1158] BSF 应该支持 CipherSuiteTLS_RSA_WITH_3DES_EDE_CBC_SHA 以及 CipherSuite TLS_RSA_WITH_AES_128_CBC_SHA。

[1159] I.6.2 BSF 的认证

[1160] BSF 由客户端如 WAP-219-TLS[30] 中指定的被认证，其进而基于 RFC 2246[6]。

[1161] BSF 证书简档应该基于 WAP 证书和 CRL 简档，如 WAP 211WAPCert[31] 定义的。

[1162] I.6.3 UE 的认证

[1163] BSF 不应该在服务器你好消息中从 UE 请求证书。BSF 应该认证 UE，如本规范 I.5.2 节指定的。

[1164] I.6.4 安全参数的建立

[1165] TLS 握手协议协商会话，其通过会话 ID 标识。客户端和 BSF 应该允许重新利用会话。会话 ID 的生存期服从 UE 和 BSF 的本地策略。推荐的生存期是五分钟。指定的最大生存期是 24 小时。

[1166] 注意，如果 BSF 坚持推荐的生存期，那么在引导重协商的情况下，UE 必然能够重新利用 TLS 会话。

[1167] 附录 J（资料性的）：

[1168] BSF 中带有本地策略加强的 USS 的使用

[1169] 本附录描述了 BSF 中本地策略加强如何被用在 NAF 和 BSF 之间以控制密钥传递到 NAF。

[1170] J.1 综述

[1171] BSF 可以具有用于零个或多个 NAF 的本地策略，其中用于 NAF 的策略可以声明用户的 GUSS 应该包括一个或多个由 GSID 标识的 USS。换句话说，对于特定的 NAF，BSF 可以要求再多一个的 USS 存在于用户 GUSS 中。

[1172] 通常，具有两个网元，其中基于某本地策略的访问控制被加强，即 NAF 和 BSF。因此必须覆盖具有基于 USS 的访问控制的两个阶段：

[1173] 1)NAF 内用于 Ua 请求的访问控制：在 NAF 中决定（并且可能在 USS 的帮助下）是否允许用户访问服务在 NAF。在从 UE 接收 B-TID 时，NAF 从 BSF 获取 NAF 专用的共享密钥 (Ks_(ext/int)_NAF)，并且选择性地获取 USS，其典型地包含 NAF 专用的永久用户身份以及授权标记。基于 NAF 中的本地策略，其可以包括评估 USS 的内容，NAF 决定用户是否被允许访问服务。

[1174] 2)BSF 内用于 Zn 请求的访问控制：在特定情况中，运营商可以希望实现 BSF 中的访问控制。此功能可以与任何 NAF 使用，但是具有这个的主要原因是为了在 NAF 处于拜访网络中的情况中实现归属运营商控制。

[1175] 本附录更详细地描述了 BSF 内用于 Zn 请求的访问控制情况。

[1176] 在使用本附录时应该注意下列事实：

[1177] -此访问控制是完全本地于 BSF 运营商的网络（即用户的归属运营商）。这隐含了对于此访问控制的实现不需要运营商间的协议。

[1178] -BSF 的本地策略可以是基于 NAF 名和 NAF 组的。为了简便，下列描述中仅提及 NAF。

[1179] J.2 使用场景

[1180] 可以确定 BSF 中的本地策略将如何工作的四个不同场景：

[1181] 1)NAF 不使用 USS（即它不从 BSF 请求 USS），并且 BSF 不具有用于此 NAF 的本地策

略。

[1182] 2)NAF 不使用 USS(即它不从 BSF 请求 USS),并且 BSF 具有用于此 NAF 的本地策略。

[1183] 3)NAF 使用 USS(即它从 BSF 请求一个或多个 USS),并且 BSF 不具有用于此 NAF 的本地策略。

[1184] 4)NAF 使用 USS(即它从 BSF 请求一个或多个 USS),并且 BSF 具有用于此 NAF 的本地策略。

[1185] 在这些场景中的每一个中执行的步骤在下列子节中更详细地描述。

[1186] 在所有场景中,NAF 已经在下列步骤执行之前通过 Ua 从 UE 参考点接收了 B-TID。步骤仅描述了关于 USS 存在的相关于 BSF 中本地策略加强的过程。而且,不相关于此访问控制的其他信息元素的传递未被提及(例如,密钥生存期、私有用户身份)。

[1187] J.2.1 场景 1 :NAF 不使用 USS,BSF 不具有用于 NAF 的本地策略

[1188] 在此场景中,NAF 不使用 USS 并且 BSF 不具有用于此 NAF 的本地策略。

[1189] 1.NAF 从 BSF 请求 NAF 专用的共享密钥。其在请求中不包括任何 GSID。

[1190] 2.BSF 使用 B-TID 在它的本地存储器中定位用户信息。

[1191] 3.BSF 检查是否存在用于 NAF 的本地策略-在此场景中不存在本地策略,即对于此特定 NAF,BSF 不要求任何 USS(由 GSID 标识的)存在于用户的 GUSS 中。

[1192] 4.BSF 衍生 NAF 专用的共享密钥,并且在响应中将它们发送到 NAF。

[1193] 5.NAF 接收带有 NAF 专用的共享密钥的响应。

[1194] 在接收到 NAF 专用的共享密钥之后,NAF 可以根据它自己的策略执行对服务的访问控制并且继续与 UE 通信。

[1195] J.2.2 场景 2 :NAF 不使用 USS,BSF 具有用于 NAF 的本地策略

[1196] 在此场景中,NAF 不使用 USS 并且 BSF 具有用于此 NAF 的本地策略。

[1197] 1.NAF 从 BSF 请求 NAF 专用的共享密钥。在请求中不包括任何 GSID。

[1198] 2.BSF 使用 B-TID 在它的本地存储器中定位用户信息。

[1199] 3.BSF 检查是否存在用于 NAF 的本地策略-在此场景中,存在用于此 NAF 的本地策略,即对于此特定 NAF,BSF 不要求任何 USS(由 GSID 标识的)存在于用户的 GUSS 中。

[1200] BSF 检查是否所有由 GSID 标识的要求的 USS 都存在于用户的 GUSS 中 :如果是,BSF 从步骤 4 继续。如果不是,则 BSF 将错误消息发送到 NAF。

[1201] 4.BSF 衍生 NAF 专用的共享密钥,并且在响应中将它们发送到 NAF。

[1202] 5.NAF 接收带有 NAF 专用的共享密钥的响应。

[1203] 在接收到 NAF 专用的共享密钥之后,NAF 可以根据它自己的策略执行对服务的访问控制并且继续与 UE 通信。

[1204] 如果 NAF 接收到“未授权”的错误消息,他可以将此消息通过 Ua 参考点向 UE 指示。在任何情况中,UE 和 NAF 间基于 GAA 的安全建立将失败,因为 NAF 没有得到 NAF 专用的共享密钥。

[1205] J.2.3 场景 3 :NAF 使用 USS,BSF 不具有用于 NAF 的本地策略

[1206] 在此场景中,NAF 使用 USS 并且 BSF 不具有用于此 NAF 的本地策略。

[1207] 1.NAF 从 BSF 请求 NAF 专用的共享密钥。在请求中包括它需要的 GSID。

[1208] 2.BSF 使用 B-TID 在它的本地存储器中定位用户信息。

[1209] 3. BSF 检查是否存在用于 NAF 的本地策略 - 在此场景中不存在本地策略，即对于此特定 NAF，BSF 不要求由 GSID 标识的 USS 存在于用户的 GUSS 中。

[1210] 4. BSF 衍生 NAF 专用的共享密钥，并且在响应中将它们和由 GSID 标识的 USS 发送到 NAF。如果在用户的 GUSS 中没有发现特定的 USS，或者 NAF 未被授权去接收特定的 USS，则这些 USS 从响应中忽略。

[1211] 5. NAF 接收带有 NAF 专用的共享密钥的响应，并且那些请求的 USS 是有效的（即，在用户的 GUSS 中发现的病情 BSF 允许由 NAF 接收的）。

[1212] 在接收到 NAF 专用的共享密钥和有效 USS 之后，NAF 可以根据它自己的策略执行对服务的访问控制（例如 USS 要求或不要求需要的授权标记）并且继续与 UE 通信。

[1213] J. 2. 4 场景 4 :NAF 使用 USS，BSF 具有用于 NAF 的本地策略

[1214] 在此场景中，NAF 使用 USS 并且 BSF 具有用于此 NAF 的本地策略。

[1215] 1. NAF 从 BSF 请求 NAF 专用的共享密钥。在请求中包括它需要的 GSID。

[1216] 2. BSF 使用 B-TID 在它的本地存储器中定位用户信息。

[1217] 3. BSF 检查是否存在用于 NAF 的本地策略 - 在此场景中存在用于此 NAF 的本地策略，即由 GSID 标识的一个或多个 USS 应该存在于用户的 GUSS 中。

[1218] BSF 检查是否所有由 GSID 标识的要求的 USS 都存在于用户的 GUSS 中 :如果是，BSF 从步骤 4 继续。如果不是，则 BSF 将错误消息发送到 NAF。

[1219] 4. BSF 衍生 NAF 专用的共享密钥，并且在响应中将它们和由 GSID 标识的 USS 发送到 NAF。如果在用户的 GUSS 中没有发现特定的 USS，或者 NAF 未被授权去接收特定的 USS，则这些 USS 从响应中忽略。

[1220] 5. NAF 接收带有 NAF 专用的共享密钥的响应，并且那些请求的 USS 是有效的（即，在用户的 GUSS 中发现的病情 BSF 允许由 NAF 接收的）。

[1221] 在接收到 NAF 专用的共享密钥和有效 USS 之后，NAF 可以根据它自己的策略执行对服务的访问控制（例如 USS 要求或不要求需要的授权标记）并且继续与 UE 通信。

[1222] 如果 NAF 接收到“未授权”的错误消息，可以将此消息通过 Ua 参考点向 UE 指示。在任何情况中，UE 和 NAF 间基于 GAA 的安全建立将失败，因为 NAF 没有得到 NAF 专用的共享密钥。

[1223] 附录 K（资料性的）:更改历史

[1224]

更改历史									
日期	TSG#	TSG Doc.	CR	Rev	Cat	主题 / 意见	旧	新	WI
2004-03	SP-23	SP-040175	-	-	D	在 TSG SA#23 上用于同意的呈现	1.2.1	2.0.0	

2004-03	SP-23	-	-	-	F	更改控制下的同意和放置（版本 6）	2.0.0	6.0.0	
2004-06	SP-24	SP-040375	001	-	F	附录 A 的移除	6.0.0	6.1.0	SEC1--SC
2004-06	SP-24	SP-040376	002	-	B	NAF 移除安全关联	6.0.0	6.1.0	SEC1--SC
2004-06	SP-24	SP-040377	003	1	D	关于事务标识符的编辑性注意的移除	6.0.0	6.1.0	SEC1--SC
2004-06	SP-24	SP-040378	004	1	B	基于 UICC 的通用引导架构的介绍	6.0.0	6.1.0	SEC1--SC
2004-06	SP-24	SP-040379	005	-	D	对 TS 33.220 的编辑性更正	6.0.0	6.1.0	SEC1--SC
2004-06	SP-24	SP-040380	006	-	C	在拜访网络中对于 NAF 的支持	6.0.0	6.1.0	SEC1--SC
2004-06	SP-24	SP-040381	007	-	C	对 TS 33.220 的编辑性更改和澄清	6.0.0	6.1.0	SEC1--SC
2004-06	SP-24	SP-040382	008	-	F	多密钥衍生规定	6.0.0	6.1.0	SEC1--SC
2004-06	SP-24	SP-040383	009	-	C	NAF 的公有主机名确认	6.0.0	6.1.0	SEC1--SC
2004-09	SP-25	SP-040619	010	-	C	密钥生存期的详细设计	6.1.0	6.2.0	SEC1-SC
2004-09	SP-25	SP-040619	011	-	C	GAA 中 USIM/ISIM 使用的细节	6.1.0	6.2.0	SEC1-SC
2004-09	SP-25	SP-040619	012	-	C	通用 Ua 接口要求	6.1.0	6.2.0	SEC1-SC

2004-09	SP-25	SP-040619	013	-	F	B-TID 生成	6.1.0	6.2.0	SEC1-SC

[1225]

2004-09	SP-25	SP-040619	014	-	B	保证 Zn 参考点的安全	6.1.0	6.2.0	SEC1-SC
2004-09	SP-25	SP-040619	015	-	D	GBA 用户安全设置	6.1.0	6.2.0	SEC1-SC
2004-09	SP-25	SP-040619	016	-	C	BSF 中 GBA_U AV 的创建	6.1.0	6.2.0	SEC1-SC
2004-09	SP-25	SP-040619	017	-	F	NAF 专用密钥默认类型定义的澄清	6.1.0	6.2.0	SEC1-SC
2004-12	SP-26	SP-040855	018	1	C	使用默认域方法的 BSF 发现	6.2.0	6.3.0	SEC1-SC
2004-12	SP-26	SP-040855	019	1	C	NAF 设置的本地合法性条件	6.2.0	6.3.0	SEC1-SC
2004-12	SP-26	SP-040855	020	3	C	GAA 中 GBA 用户安全设置 (GUSS) 使用以及 NAF 组的介绍	6.2.0	6.3.0	SEC1-SC
2004-12	SP-26	SP-040855	021	2	C	GAA 中 USIM/ISIM 选择的细节	6.2.0	6.3.0	SEC1-SC
2004-12	SP-26	SP-040855	023	-	B	用于保证 Zn′ 参考点安全的 TLS 简档	6.2.0	6.3.0	SEC1-SC
2004-12	SP-26	SP-040855	025	2	F	GBA_U 密钥衍生过程的最优化	6.2.0	6.3.0	SEC1-SC
2004-12	SP-26	SP-040855	027	2	F	用于 GBA_U 的 ME 能力要求	6.2.0	6.3.0	SEC1-SC
2004-12	SP-26	SP-040855	034	1	D	添加关于回放保护的注意	6.2.0	6.3.0	SEC1-SC

2004-12	SP-26	SP-040855	035	1	C	完成用于 GBA_U 的 MAC 修改	6.2.0	6.3.0	SEC1-SC
2004-12	SP-26	SP-040855	036	1	F	非必需编辑性注意的移除	6.2.0	6.3.0	SEC1-SC
2004-12	SP-26	SP-040855	038	1	C	运行在 BSF 和 HSS 间每个 Zh 上的仅有的一个 AV 的获取	6.2.0	6.3.0	SEC1-SC
2004-12	SP-26	SP-040855	039	1	B	TS 33.220 的整理	6.2.0	6.3.0	SEC1-SC
2004-12	SP-26	SP-040855	040	1	F	基于 ME 的 GBA 密钥的新密钥管理	6.2.0	6.3.0	SEC1-SC

[1226]

2004-12	SP-26	SP-040855	041	1	C	密钥衍生函数	6.2.0	6.3.0	SEC1-SC
2004-12	SP-26	SP-040855	042	1	D	密钥到重协商	6.2.0	6.3.0	SEC1-SC
2004-12	SP-26	SP-040855	043	1	C	版本 6 中非 GUSS/USS 更新过程	6.2.0	6.3.0	GBA-SSC
2004-12	SP-26	SP-040855	044	1	C	阐明每 NAF-Id 存储在 UE 中 NAF 专用密钥的数量	6.2.0	6.3.0	SEC1-SC
2005-03	SP-27	SP-040139	045	1	F	密钥衍生函数 :字符编码	6.3.0	6.4.0	SEC1-SC
2005-03	SP-27	SP-040139	047	1	D	引导时间戳	6.3.0	6.4.0	SEC1-SC
2005-03	SP-27	SP-040139	048	-	F	GBA_U NAF 衍生过程中 B-TID 的存储	6.3.0	6.4.0	SEC1-SC

2005-06	SP-28	SP-050262	050	1	F	BSF 中用于本地策略加强的 USS 的使用	6.4.0	6.5.0	SEC1-SC
2005-06	SP-28	SP-050262	051	1	F	更正图 4.4	6.4.0	6.5.0	SEC1-SC
2005-06	SP-28	SP-050263	052	-	B	GBA 用户安全设置 (GUSS) 传输优化	6.4.0	7.0.0	SEC1-SC
2005-09	SP-29	SP-050553	0054	-	A	GBA 中对 NAF 匿名访问的澄清	7.0.0	7.1.0	SEC1-SC
2005-09	SP-29	SP-050554	0056	-	A	从 USS 移除 IMPI	7.0.0	7.1.0	SEC1-SC
2005-09	SP-29	SP-050572	0057	-	C	关于 BSF 中用于本地策略加强的 USS 的使用的资料性附录	7.0.0	7.2.0	SEC1-SC
2005-09	SP-29	SP-050557	0059	-	A	移除涉及 BSF 寻址的文本复本	7.0.0	7.1.0	SEC-SC1
2005-09	SP-29	SP-050555	0061	-	A	衍生密钥生存期的澄清	7.0.0	7.1.0	SEC1-SC
2005-09	SP-29	SP-050575	0062	-	B	密钥选择机制的介绍	7.0.0	7.2.0	SEC1-SC
2005-09	SP-29	SP-050556	0064	-	A	用于多 HSS 部署的 Dz 接口的添加	7.0.0	7.1.0	SEC1-SC

[1227]

2005-09	SP-29	SP-050565	0066	-	A	移除对于批量发送认证向量的要求	7.0.0	7.1.0	GBA
2005-09	SP-29	SP-050551	0068	-	A	关于编码用于 GBA_U NAF 衍生过程的输入参数的澄清	7.0.0	7.1.0	SEC1-SC

2005-09	SP-29	SP-050577	0069	1	B	关于 2G GBA 的标准化附录	7.0.0	7.1.0	2G GBA
2005-09	SP-29	SP-050552	0071	-	A	提供基于 Ua 安全协议的密钥分离	7.0.0	7.1.0	SEC1-SC
2005-10	post SP-29	-	-	-	-	基于 SP-29 上的 CR 对于版本 6 和版本 7 间排列附录的编辑性更改	7.1.0	7.1.1	

[1228] 附录 C

[1229] 3GPP TS 29.109 V7.0.0(2005-09)

[1230] 技术报告

[1231] 第三代伙伴计划；

[1232] 技术规范组核心网和终端；

[1233] 通用认证架构 (GAA)；

[1234] 基于直径协议的 Zh 和 Zn 接口；阶段 3

[1235] (版本 7)

[1236] 本文档已经在第三代伙伴计划 (3GPP™) 中开发并且可以针对 3GPP 的意图进一步详细阐述。

[1237] 本文档还没有经过 3GPP 组织伙伴的任何同意处理过程并且尚未实现。

[1238] 提供此规范仅在 3GPP 内部用于进一步的开发工作。组织伙伴不接受对于使用此规范的任何义务。

[1239] 对于 3GPP™ 系统实现的规范和报告应该通过 3GPP 组织伙伴的出版办公室获得。

[1240] 关键字

[1241] UMTS,网络,协议

[1242] 3GPP

[1243] 通信地址

[1244] 3GPP 支持办公室地址

[1245] 650 Route des Lucioles-Sophia Antipolis

[1246] Valbonne-FRANCE

[1247] Tel. :+33492944200 Fax :+33493654716

[1248] 因特网

[1249] http://www.3gpp.org

[1250] 版权声明

[1251] 除了通过书面许可的授权没有部分可以复制。版权和前述限制扩展到所有媒体中的复制。

[1252] © 2005,3GPP Organizational Partners(AR1B,ATIS,CCSA,ETSI,TTA,TTC)。

[1253] All rights reserved

[1254] 目录

[1255] 1 范围 4
[1256] 2 参考 7
[1257] 3 定义、符号和缩略语 7
[1258] 3.1 定义 7
[1259] 3.2 符号 8
[1260] 3.3 缩略语 9
[1261] 4 GBA 引导 Zh 接口 10
[1262] 4.1 通用引导网络架构 10
[1263] 4.2 BSF 和 HSS 间的协议 Zh 10
[1264] 5 GBA 应用 Zh 接口 14
[1265] 5.1 应用的网络架构 14
[1266] 5.2 BSF 和 HSS 间的协议 Zn 14
[1267] 6 用于 Zh 和 Zn 接口的直径协议 17
[1268] 6.1 命令码值 17
[1269] 6.2 结果码值 17
[1270] 6.2.1 成功 17
[1271] 6.2.2 永久性失败 18
[1272] 6.2.2.1 DIAMETER_ERROR_IMPI_UNKNOWN(5401) 18
[1273] 6.2.2.2 DIAMETER_ERROR_NOT_AUTHORIZED(5402) 18
[1274] 6.2.2.3 DIAMETER_ERROR_TRANSACTION_IDENTIFIER_INVALID(5403) 18
[1275] 6.2.2.4 空 18
[1276] 6.2.2.5 空 18
[1277] 6.2.2.6 空 18
[1278] 6.2.2.7 空 18
[1279] 6.3 AVP 19
[1280] 6.3.1 公共 AVP 19
[1281] 6.3.1.1 GBA-UserSecSettings AVP 19
[1282] 6.3.1.2 事务 - 标识符 AVP 19
[1283] 6.3.1.3NAF- 主机名 19
[1284] 6.3.1.4 GAA- 服务 - 标识符 AVP 20
[1285] 6.3.1.5 密钥 - 到期时间 AVP 20
[1286] 6.3.1.6 ME- 密钥 - 资料 AVP 20
[1287] 6.3.1.7 UICC- 密钥 - 资料 AVP 20
[1288] 6.3.1.8 GBA_U- 察觉 - 指示符 20
[1289] 6。3.1.9 BootstrapInfoCreationTime AVP 20
[1290] 6.3.1.10 GUSS- 时间戳 AVP 20
[1291] 6.4 到 HSS 的用户身份解析 20
[1292] 7 名字空间的使用 22

[1293] 7.1 AVP 代码 22
[1294] 7.2 实验性 - 结果 - 码 AVP 值 22
[1295] 7.3 命令码值 22
[1296] 附录 A(标准化的) :GBA-UserSecSettings XML 定义 23
[1297] 附录 B(标准化的) :GAA 服务类型码 26
[1298] 附录 C(标准化的) :GAA 授权标记码 26
[1299] 附录 D(资料性的) :更改历史 27

[1300] 前言

[1301] 此技术报告已经由第三代伙伴计划 (3 GPP) 制作。

[1302] 本文档的内容服从 TSG 中的连续工作并且可以随着正式的 TSG 同意改变。一旦 TSG 修改本文档的内容，TSG 将通过带有发布日期和如下增加的版本号的可识别变化来对其进行重新发布 :

[1303] 版本 x. y. z

[1304] x 第一个数字

[1305] 1 呈现给 TSG 用于信息

[1306] 2 呈现给 TSG 用于同意

[1307] 3 或者更大指示修改控制下的 TSG 同意文档

[1308] y 第二个数字增大用于所有实质的修改，即技术增强、修正、更新等。

[1309] z 当仅编辑性修改已经合并于该文档中时第三个数字增大。1 范围

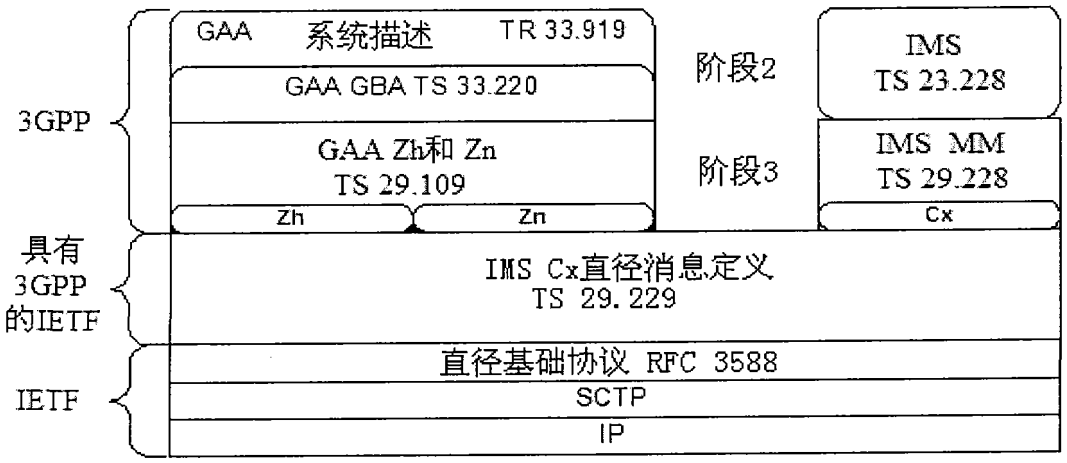
[1310] 本第 3 阶段规范定义了用于引导 BSF 的 HSS 解析的 Zh 接口 (BSF-HSS) 和 Dz 接口 (BSF-SLF) 的基于直径的实现，以及通用认证架构 (GAA) 中的 GAA 应用 Zn 接口 (BSF-NAF)。该定义包含过程、消息内容和编码。用于引导的过程和引导的安全关联的使用定义于 TS33.221[5] 中。

[1311] 此规范是通用认证架构 (GAA) 规范系列的一部分。

[1312] 基于直径的最初实现是基于 CSCF 和 HSS 间 Cx 接口多媒体 -Auth- 请求 / 应答消息的重用。这些消息定义于 3GPP TS 29.229[3]。3GPP IMS 移动性管理使用 CSCF 和 HSS 间的相同定义。本文档定义定义的消息如何与引导和 GAA 应用过程 (例如，用户证书) 以及 GAA 网元中 (BSF、HSS 和 NAF) 需要的应用逻辑一起使用。

[1313] 图 1.1 描述了这些规范与其他规范的关系。

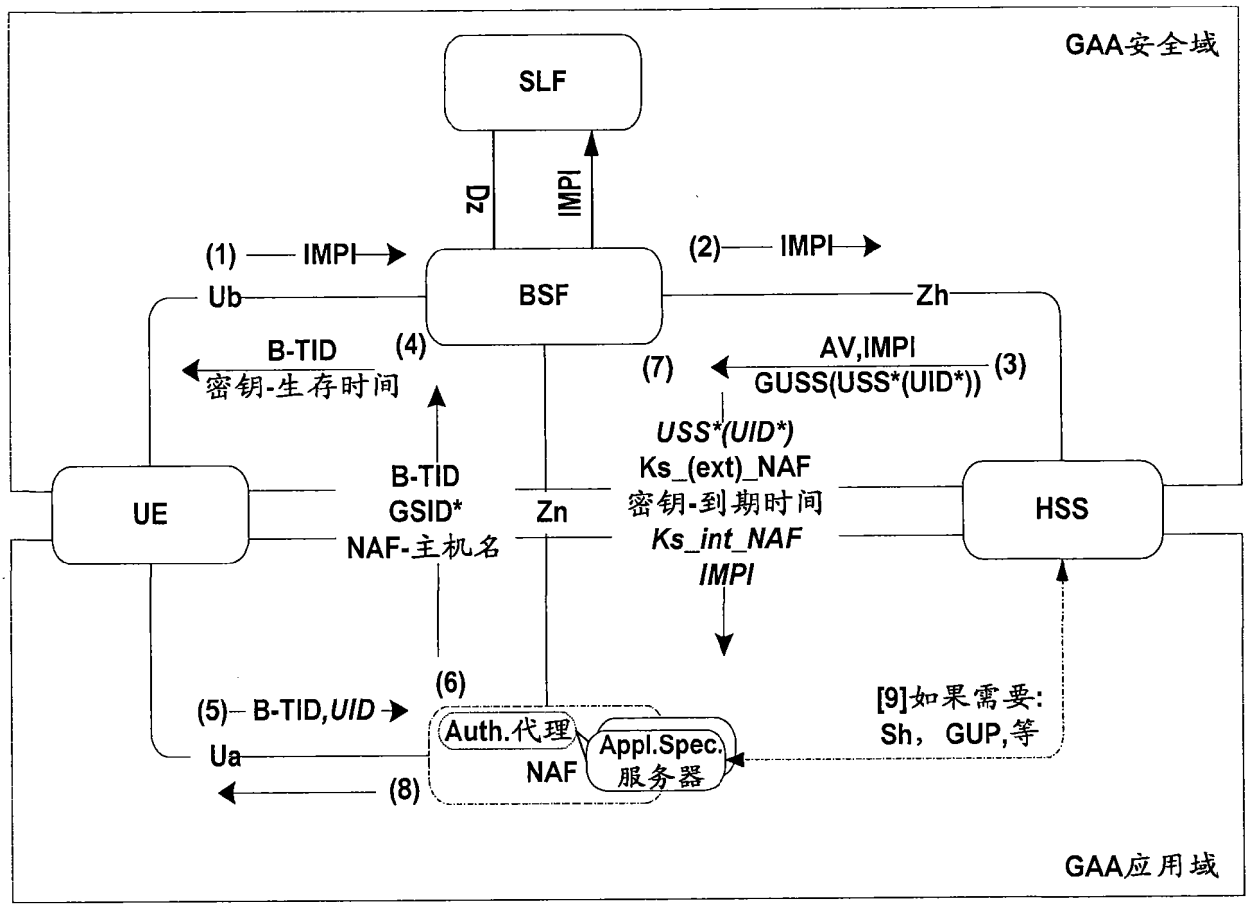
[1314]



[1315] 图 1.1 :与其他规范的关系

[1316] 图 1.2 提供了 GAA 系统中整个信令过程的非正式全面快速介绍。重要标识符以粗体标记,并且可选日期条目是斜体的。没有定义于此 TS 中的 Ub 和 Ua 接口被简化。

[1317]



粗体=重要身份。 斜体=可选条目。 Ub和Ua接口被简化。

[1318] 图 1.2 GAA 系统中整个信令过程

[1319] 2 参考

[1320] 下列文档包含通过此文本中的参考的规定,组成本文档的规定。

[1321] 参考是特定的（由出版日期、印刷号、版本号等识别）或非特定的。

[1322] 对于特定参考，后续修改不适用。

[1323] 对于非特定参考，应用最新版本。在参考 3 GPP 文档（包括 GSM 文档）的情况中，非特定参考隐含地指与当前文档具有相同版本的文档的最新版本。

[1324] IETF RFC 3588，″ Dlameter Base Protocol″ .

[1325] 3GPP TS 29.228：″ IP Multimedia(1M)Subsystem Cx and Dx Interfaces；Signalling flows andmessage contcnts″ .

[1326] 3GPP TS29.229：″ Cx and Dx interfaces based on the Diameter protocol″ .

[1327] 3GPP TR 33.919 ″ Generic Authentication Architecture(GAA)；System Description(rel-6)″ .

[1328] 3GPP TS 33.220 ″ Gencric Authentication Architecture(GAA)；Generic Bootstrapping Architccture(rel-6)″ .

[1329] 3GPP TS 33.221″ Generlc Authentication Architecture(GAA)；Support for Subacriber Certificates(rel-6)″ .

[1330] 3GPP TS 24.109：″ Bootstrapping intarface(Ub)and Nerwork application function interface(Ua)；Protocol details″ .

[1331] 3GPP TS 29.230： ″ Diomcter applications；3GPP specific codes and identifiers(rel-6)″

[1332] IETF RFC 3589： ″ Diameter Command Codes for Third Generation Partnership Project(3GPP)Rclease5″ .

[1333] 3GPPTS 23.008：″ Organisation of subscrtber data″

[1334] 3GPP TS33.222：″ Geberic Authertication Architecture(GAA)；Access to network applicationtunctions using secure hypertext transfcr protocol(HTTPS)(rel-6)″ .

[1335] 3GFP TS 23.228：″ IP Multimedia Subsystem(IMS)；Stage2″

[1336] 3 定义、符号和缩略语

[1337] 3.1 定义

[1338] 出于本文档的目的，3GPP TS 23.008[10]、3GPP TR 33.919[4]、3GPPTS 33.220[5] 中给出的术语和定义与下列增加一起应用。

[1339] 引导信息：BSF 中的引导信息（引导的数据）包括引导事务标识符 (B-TID)、密钥资料 (Ks)、密钥生存期（到期时间）、boostrapinfo 创建时间、IMPI 和带有 BSF 控制信息的 GUSS（如果从 HSS 接收了）。

[1340] GAA 应用：GAA 应用是使用由 GBA 引导过程创建的安全关联的应用。

[1341] GAA 服务：GAA 服务是使用由 GBA 引导过程创建的安全关联的运营商特定终端用户服务。GAA 服务通过 GAA 服务标识符进行标识。GAA 服务使用一些由 GAA 应用类型定义的标准化的或者专有 GAA 应用。

[1342] NAF 专用引导信息：从 BSF 传输到 NAF 的 NAF 专用引导信息包含 NAF 和它的来自于引导的数据的服务特定部分以及衍生自引导数据的所需密钥信息。

[1343] 服务 / 应用：术语服务在此使用它的普通含义。服务是 MNO 提供给用户的事物。

GAA 服务通过 GAA 服务标识符 (GSID) 标识。在阶段 2 文档 ([4]、[5]、[6] 和 [11]) 中，术语应用以相同的含义使用，即 MNO 向用户提供应用。存在一个原因避免这里的术语应用的使用。在直径中，应用已经是保留术语。在直径中，应用通过应用标识符标识。

[1344] 3.2 符号

[1345] 出于本文档的目的，在 3GPP TS 23.008[10] 中给出术语和定义。

[1346] 3.3 缩略语

[1347] 出于本文档的目的，应用下列缩略语 ：

[1348] AK 匿名密钥

[1349] AKA 认证和密钥协议

[1350] AUTN 认证记号

[1351] AV 认证向量。3 GPP AV = [RAND，AUTN，XRES，CK，IK].

[1352] AVP 直径消息中的属性 - 值 - 对

[1353] BIA BootstrappingInfo- 应答消息

[1354] BIR BootstrappingInfo- 请求消息

[1355] BS 引导过程

[1356] BSF 引导服务器功能

[1357] BSF 是在 MNO 的控制下受网元主控。

[1358] B-TID 引导事务标识符

[1359] CA 证书机构

[1360] CK 机密性密钥

[1361] FQDN URJ 中的全资格域名 (例如 http://FQDN:80)

[1362] GAA 通用认证架构

[1363] GBA 通用引导架构

[1364] GSID GAA 服务标识符

[1365] GUSS GBA 用户安全设置

[1366] HSS 归属用户系统

[1367] IK 完整性密钥

[1368] IMPIIP 多媒体私有身份

[1369] IMPU IP 多媒体公有身份

[1370] Ks 密钥资料

[1371] Ks_ext_NAF 用于特定 NAF 的基于 ME 的密钥

[1372] MNO 移动网络运营商

[1373] NAF 运营商 - 控制的网络应用功能功能性

[1374] NAF 是在 MNO 的控制下网元中的主机。

[1375] RAND 认证中的随机质询

[1376] REQ 在直径头中指示消息是请求

[1377] SCTP 流控制传输协议

[1378] SLF 订阅位置功能

[1379] SSC 用户证书功能

[1380] Ua 用于 GAA 应用的 UE-NAF 接口

[1381] Ub 用于引导的 UE-BSF 接口

[1382] UE 用户设备

[1383] Ks_int_NAF 用于特定 NAF 的基于 UICC 的密钥

[1384] USS 用户安全设置 (GUSS 的一部分)

[1385] XRES 认证中的期望响应

[1386] Zh 用于引导过程的 BSF-HSS 接口

[1387] Zn 用于应用的 GAA BSF-NAF 接口

[1388] 4 GBA 引导 Zh 接口

[1389] 4.1 通用引导网络架构

[1390] 引导过程的网络架构呈现于图 4.1 中。接口 Ub(引导) 定义于 3GPPTS 24.109[7] 中并且接口 Zh 在此规范中。

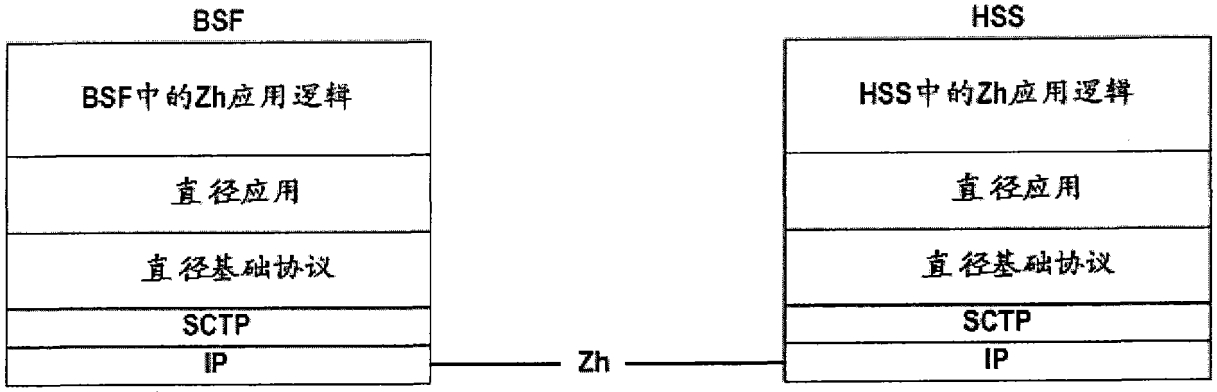
[1391]



[1392] 图 4.1 引导过程的网络架构

[1393] 引导过程中 Zh 接口的协议栈呈现于图 4.2 中。直径基础协议定义于 [1] 中并且直径应用在 3GPP TS 29.229[3] 中。对于 Zh 接口的要求定义于 3GPP TS 33.220[5] 中

[1394]



[1395] 图 4.2 Zh 接口的协议栈

[1396] 4.2 BSF 和 HSS 间的协议 Zh

[1397] 对于 Zh 接口的要求定义于 3GPP TS 33.220[5] 中。

[1398] 引导 Zh 接口从 HSS 执行认证向量和可能 GBA 用户安全设置的获取。全面引导过程在图 4.3 中描述。基本过程是 :

[1399] A) 通过协议 Ub, UE 开始与给出用户的 IMPI 的 BSF 的引导过程 (见 3GPP TS 24.109[7])。

[1400] B)BSF 开始与用户的 HSS 开始协议 Zh

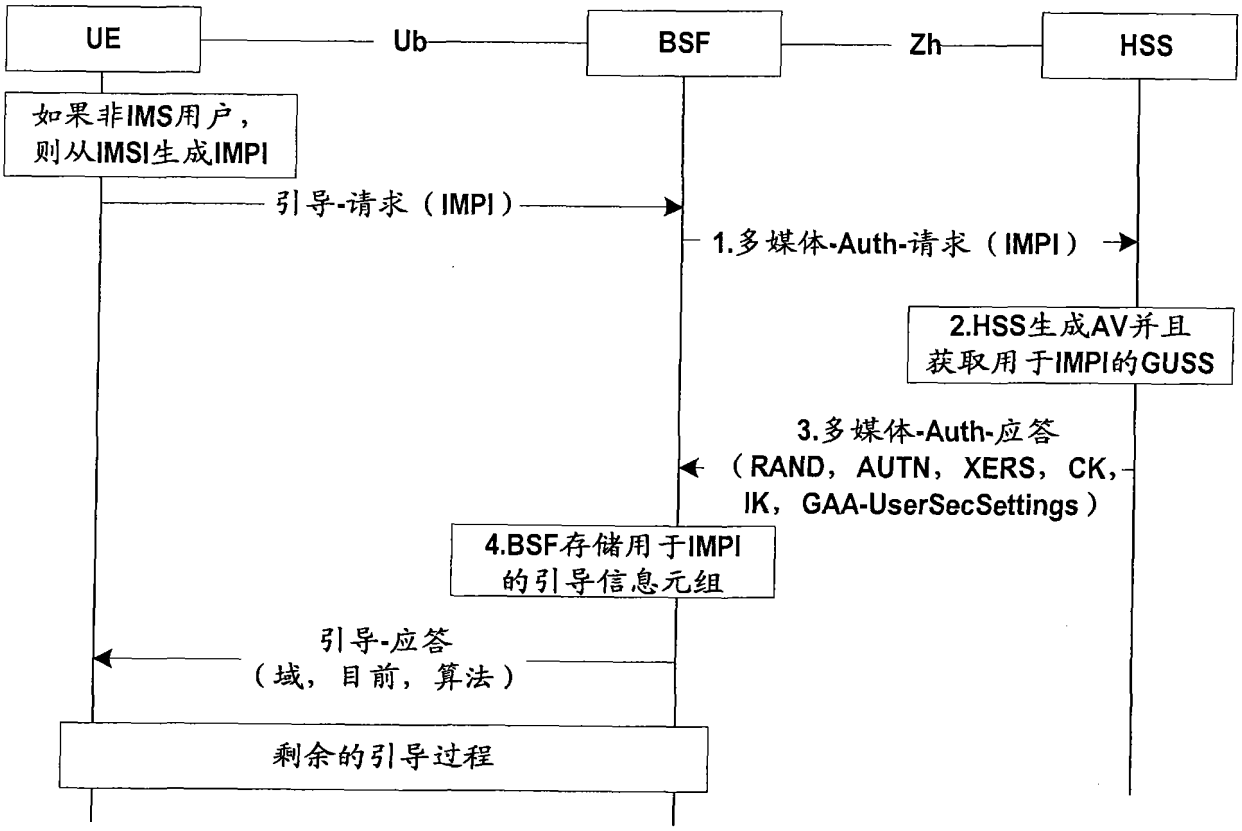
[1401] ● BSF 请求用户的认证向量和对应于 IMPI 的 GBA 用户安全设置 (GUSS)。

[1402] ● HSS 向 BSF 提供请求的认证向量和 GUSS(如果有)

[1403] 注意：如果网络内部署有多于一个的 HSS，则在向 HSS 发送信息的请求之前 BSF 必须使用 Dz 接口联系 SLF（见 6.4 节）。

[1404] C)BSF 继续与 UE 的协议 Ub（见 3GPP TS 24.109[7]）。

[1405]



[1406] 图 4.3 GBA 引导过程

[1407] 图 4.3 中的引导过程的步骤是：

[1408] 步骤 1

[1409] BSF 应该以多媒体 -Auth- 请求 (MAR) 消息的格式将下列引导 - 请求发送到 HSS。下面以与 3GPP TS 29.229[3] 中相同的格式给出了消息内容。大括号指示了强制的 AVP。方括号指示可选的 AVP。“的地址”指全资格主机名 (FQDN)。

[1410] <Multimedia-Auth-Requeat>:: = <Diameter Header :303, REQ, PXY, 16777221>

[1411] <Session-Id>

[1412] {Vendor-Specific-Application-Id }

[1413] {Auth-Session-State} ;No_STATE_MAINTAINED

[1414] {Origin-Host} ;Addreas of BSF

[1415] {Origin-Realm} ;Realm of BSF

[1416] {Cestination-Realm} ;Realm of HSS

[1417] {Cestination-Host} ;Address of the HSS

[1418] {User-Name} ;IMPr from UE

[1419] {CUSS-Timestamp} ;Timestamp of GUSS in

BSF

[1420] *{AVP}

[1421] *{Proxy-Info}

[1422] *{Route-Record}

[1423] 根据[1]的强制的供应商-特定-应用-ID内容是：

[1424] <Vendor-Specific-Application-Id>:: = <AVP header* 260>

[1425] 1*{Vendor-Id} ;3GPPi310415

[1426] 0*1{Aoth-Appllcation-Id} ;16777221

[1427] 0*1{Acct-Application-Id} ;Omitted

[1428] 当确定目的地-主机AVP的值时，如果需要，BSF可以使用转向器(redirector)功能(SLF)以解析HSS的地址(见3GPP TS 29.229[3])。根据3GPP TS 29.229[3]BSF应该将Auth会话状态设置为NO_STATE_MAINTAINED以通知HSS不需要为此会话保持任何状态信息。用户-名是如3GPP TS 29.228[2]中要求的IMS私有用户身份(IMPI)。如果BSF支持GUSS时间戳机制并且具有GUSS的本地副本(其具有时间戳)，则BSF可以包括GUSS-时间戳AVP。在此情况中，GUSS-时间戳AVP应该包含来自于用户的GUSS的时间戳。否则GUSS-时间戳AVP将不存在。

[1429] 步骤2

[1430] 当HSS接收到MAR消息时，HSS将根据IMPI衍生用户认证向量(AV)信息并且将它装入在3GPP TS 29.229[3]中定义的SIP-Auth-数据AVP中。如果存在用于IMPI的GUSS，则HSS应该完成下列之一：

[1431] 1.如果BSF支持GUSS时间戳机制并且在MAR消息中接收了GUSS-时间戳AVP，那么它将把HSS中的GUSS时间戳与接收的时间戳进行比较。

[1432] -如果时间戳相等，那么它应该将静态字符串“GUSS时间戳相等”装入GBA-UserSecSettings AVP。

[1433] -如果没有接收到GUSS-时间戳AVP，或者时间戳不相等，那么它应该使用GUSS装入GBA-UserSecSettings AVP。

[1434] 2.如果HSS不支持GUSS时间戳机制，它将使用GUSS装入GBA-UserSecSettings AVP。

[1435] Zh接口中的MAR/MAA序列绝对不能改变HSS中可能同时进行的IMS MM应用会话的可能状态信息。

[1436] 如果来自于BSF的用户-名(IMPI)对于HSS全部未知，则出现错误情况5401。

[1437] 步骤3

[1438] HSS将以多媒体-Auth-应答(MAA)消息的格式将下列引导-应答消息发回到BSF。

[1439] <Multimedia-Auth-Answer>:: = <Diameter Header :303，PXY，16777221>

[1440] <Session-ld>

[1441] {Vendor-Speclfic-Appllcation-Id}

[1442] {Result-Code}

[1443] {Experimental-Rcsult}

[1444] {Auth-Session-State} ;NO_STATE_MAINTAINED

[1445] {Origin-Realm} ;Realm of HSS

[1446] *{SIP-Auth-Data-Item}

[1447] {GaA-UserSecSettinga} ;GUSS

[1448] *{AVP}

[1449] *{Route-Record}

[1450] HSS应该设置强制Auth-会话-状态AVP为NO_STATE_MAINTAINED,因为HSS不保留关于此会话的任何状态信息并且BSF不需要发送任何会话终止请求3GPP TS 29.229[3]。用户-名AVP(IMPI)可以被发送回去用于检查。要求的认证向量在SIP-Auth-数据-条目AVP中发送。用户的所有GAA应用的安全设置在GBA-UserSecSettings AVP中发送。

[1451] 步骤4

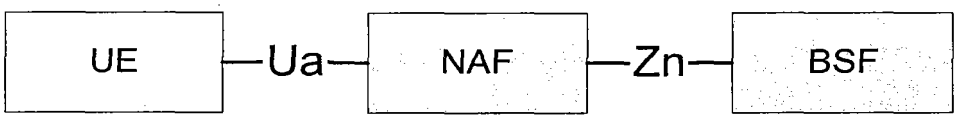
[1452] 当BSF接收到MAA消息时,BSF从机密性密钥(CK)和完整性密钥(IK)如3GPP TS 33.220[5]中描述的生成需要的密钥资料(Ks)并且为临时存储元组<IMPI,Ks,GBA-UserSecSettings>以供GAA应用中进一步的使用。Ub接口中的引导过程的剩余部分也将稍后将引导事务标识符(B-TID)添加到元组作为密钥和密钥生存期(到期时间)。如果BSF在步骤1中发送GUSS-时间戳AVP,并且如果GBA-UserSecSettings AVP包含静态字符串“GUSS时间戳相等”,那么BSF中的GUSS本地副本应该保存。如果GBA-UserSecSettings AVP不存在于MAA消息中,则GUSS的本地副本应该删除。如果GBA-UserSecSettings AVP包含新的GUSS,则GUSS的本地副本应该删除,并且在BSF中应该存储新的GUSS。

[1453] 5 GBA应用Zh接口

[1454] 5.1应用的网络架构

[1455] GAA应用过程的网络架构呈现于图5.1中。3GPP GAA应用列出于附录B中。不同的GAA应用可以以不同的方式实现Ua接口。Zn接口在此规范中定义。

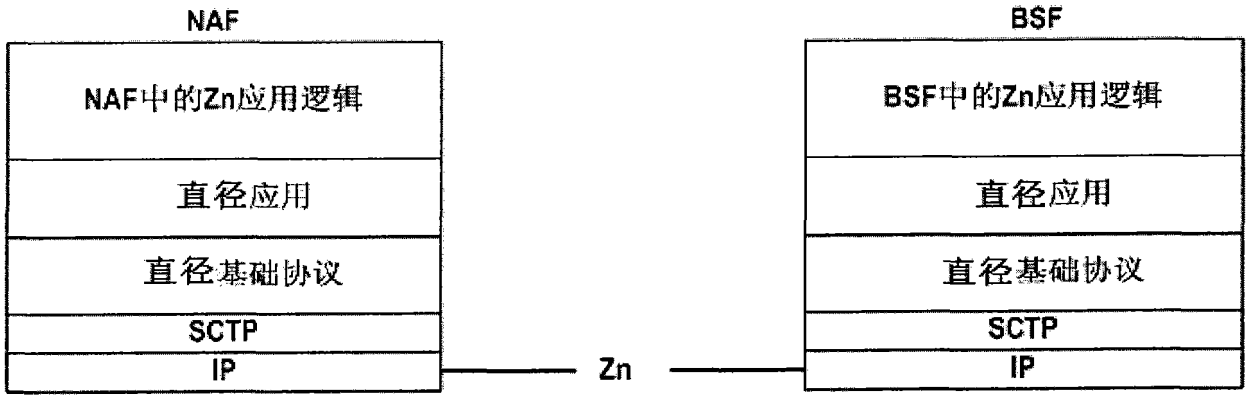
[1456]



[1457] 图5.1 GAA应用的网络架构

[1458] 用于GAA应用的Zn接口的协议栈呈现于图5.2中。直径基础协议定义于[1]中并且直径应用定义在3GPP TS 29.229[3]中。对于Zn接口的要求定义于3GPP TS 33.220[5]中。

[1459]



[1460] 图 5.2 Zn 接口的协议栈

[1461] 5.2 BSF 和 HSS 间的协议 Zn

[1462] 对于 Zn 接口的要求定义于 3GPP TS 33.220[5] 中。

[1463] 协议 Zn 通过 NAF 从 BSF 检索密钥资料和可能的用户安全设置数据。在 UE 使用 BSF 被认证后，每次 UE 希望与 UE 交互，则如图 5.3 中描述的执行下列步骤。基本过程是：

[1464] A)UE 开始协议 Ua（见 3GPP TS 33.220[5]）

[1465] 通常 UE 和 NAF 仍将不共享保护协议 Ua 所要求的密钥。如果它们已经共享了，则不需要 NAF 调用协议 Zn。

[1466] 假设 UE 向 NAF 提供足够的信息，即引导事务标识符 (B-TID)，以允许 NAF 从 BSF 检索特定的密钥资料（例如，GBA_ME 情况中的 Ks_NAF，以及 Ks_ext_NAF 或者 Ks_int_NAF 或者 GBA_U 的情况中的两者）。

[1467] UE 从密钥资料衍生保护协议 Ua 所要求的密钥。

[1468] B)NAF 与 BSF 开始协议 Zn

[1469] NAF 请求 NAF 专用密钥资料，该密钥资料对应于在协议 Ua 的开始时 UE 向 NAF 提供的信息（即引导事务标识符）。

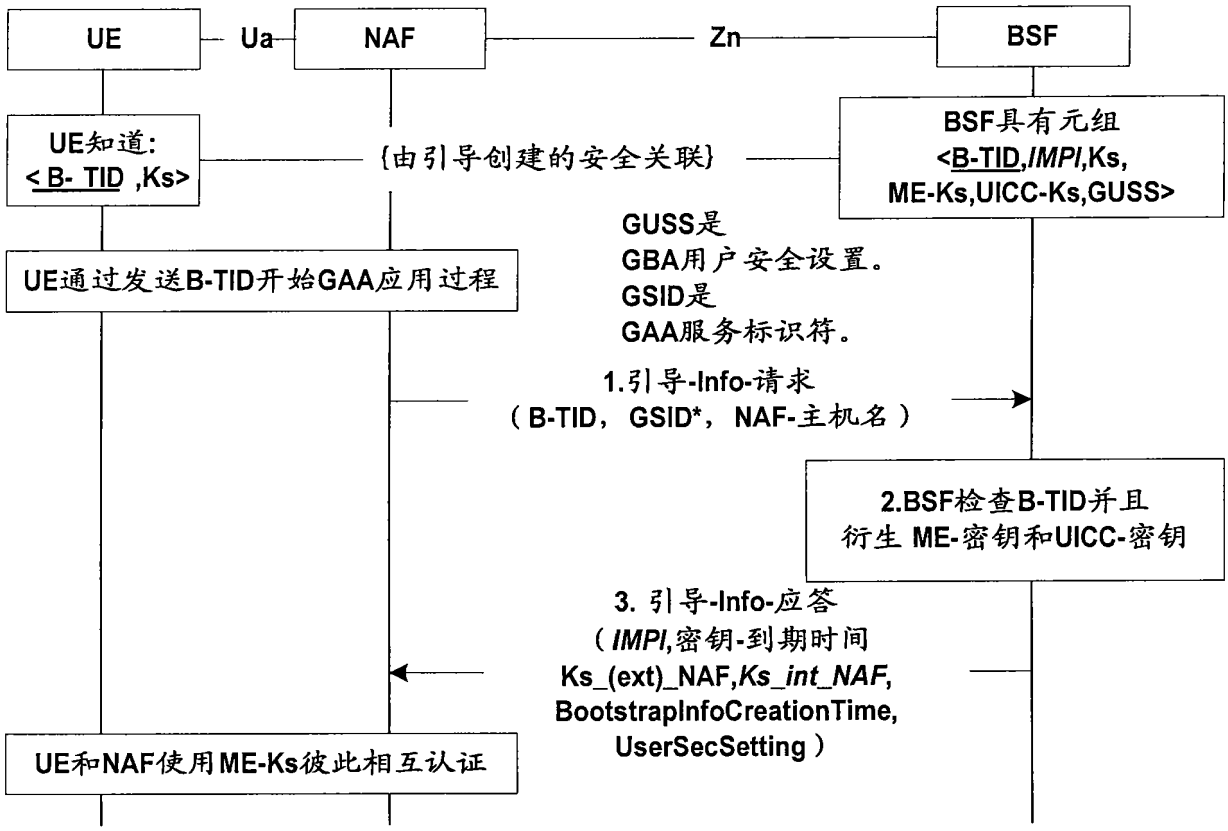
[1470] BSF 生成并向 NAF 提供请求的 NAF 专用密钥资料、到期时间、bootstrapinfo 创建时间和定义用于接收的应用标识符的适当的用户安全设置。

[1471] C)NAF 与 UE 继续协议 Ua（见 3GPP TS 33.221[6]）

[1472] 一旦协议 Ua 的运行完成，就达到了引导的目的，因为它使 UE 和 NAF 能够以安全的方式运行协议 Ua。

[1473] 普通 GAA 应用过程呈现于图 5.3 中。

[1474]



[1475] 图 5.3 GAA 应用过程

[1476] 图 5.3 中 GAA 应用过程的步骤是 :

[1477] 步骤 1

[1478] NAF 应该将引导 -Info- 请求消息 (BIR) 发送到BSF。在这里,消息的内容以与 3GPP TS 29.229[3] 中相同的格式给出。大括号指示强制 AVP。方括号指示可选 AVP。地址指全资格主机名 (FQDN)。

[1479] <Sootstrapping-Info-Request>:: = <Diameter Header :310, REO, PXY, 16777220>

[1480] <Session-Id>

[1481] {Vondor-Speclfic-Application-Id}

[1482] {Origin-Host} ;Address of NAF

[1483] {origin-Reain} ;Realm of NAF

[1484] {Oestination-Realm } ;Realm of BSF

[1485] {Oestination-Rost} ;Addrdss of the BSF

[1486] *{GAA-Service-Identirier} ;Service identifiers

[1487] {Transaction-Identifier} ;B-TID

[1488] {NAF-Hostname} ;FooN of NAF as seen by UE

[1489] {GBA_U-Awarenesa-Indicator} ;GBA_U awareness of the NAF

[1490] *{AVP}

[1491] *[Proxy-Info]

[1492] *{ Route-Record}

[1493] 根据 [1] 的提供商 - 特定 - 应用 -ID 内容是 :

[1494] <Yendor-Specific-Application-Id>:: = <AVP header :260>

[1495] 1* {Vendor-Id} ;3GPP is 10415

[1496] 0*1{Auth-Application-Id} ;16777220

[1497] 0*1{Acct-Application-Id} ;Gmitted

[1498] 设置目的地 - 域 AVP 为用户的 BSF。BSF 的地址从 B-TID 提取。

[1499] 注意 :在其中用户已经联系了位于拜访网络中的 NAF 的情况中，NAF 通过位于与 NAF 相同的网络中的直径 - 代理 (D-Proxy) 联系用户的归属 BSF。本地 BSF 和 D-Proxy 可以共同定位。见 3GPP TS 33.220[6]。

[1500] NAF 指示了由 GAA- 服务 - 标识符 AVP 针对其获取信息的 GAA 服务。引导事务标识符定义更早的引导过程执行。

[1501] 步骤 2

[1502] 在成功的情况中，BSF 具有由引导事务标识符 (B-TID) 标识的元组 <B-TID，IMPI，Ks，密钥生存期，Bootstrapinfo 创建时间，GBA-UserSecSettings>。当 BSF 接收到请求时，它检查用于给定 B-TID 元组的存在和有效性。如果检查失败，则 BSF 发送带有实验性 - 结果集合的应答消息以指示错误类型 5403。如果用于 B-TID 的元组存在，但是到期了，则还发送错误类型 5403 以指示对于引导过程恢复的需要。在成功的情况中，结果 - 码被设置为定义于 [1] 中的 2xxx。

[1503] BSF 根据 B-TID 衍生用于 ME 的密钥资料 (即 GBA ME 情况中的 Ks_NAF，GBA_U 情况中的 Ks_ext_NAF) 和用于 UICC 的可能密钥资料 (即 GBA_U 情况中的 Ks_int_NAF)，并且将它们打包到 ME- 密钥 - 资料 AVP 和可能的 UICC- 密钥 - 资料 AVP 中。ME- 密钥 - 资料包含 Ks_(ext)_NAF 并且 UICC- 密钥 - 资料 AVP 包含 Ks_int_NAF 密钥。根据对 GBA-UserSecSettings AVP 请求的 GAA- 服务 - 标识符 AVP，BSF 选择正确的用户安全设置。如果 NAF 分组由运营商使用并且存在一个或多个相应于请求的 GSID 的 USS，那么还检查 USS 的 nafGroup 属性。如果 NAF 已经发送了不具有相应用户安全设置的 GAA- 服务 - 标识符，并且本地配置 BSF 以拒绝那些来自于 NAF 的请求，那么出现错误 5402。如果 NAF 已经发送了具有相应用户安全设置的 GAA- 服务 - 标识符，但是本地配置 BSF 以拒绝那些来自于 NAF 的请求，那么也出现错误 5402。

[1504] 可以通过不同的 FQDN 从 UE 对 NAF 进行寻址。BSF 应该检查此 NAF- 主机名是否被允许用于 NAF。如果在 BSF 中配置的由它的起源 - 主机 AVP 标识的 NAF 没有被授权使用给定的 NAF- 主机名，则 BSF 可以出现错误 5402。也可以配置 BSF 以便特定 NAF 不被授权使用特定的 GAA- 服务 - 标识符。这个情况也可以由错误码 5402 指示。

[1505] 步骤 3

[1506] 在那之后 BSF 将引导 -Info- 应答消息 (BIA) 发回到 NAF。

[1507] <Boostrapping-Info-Answer>:: = <Diameter Header :310，PXY，16777220>

[1508] <Session-Id>

[1509] {Vendor-Specific-Application-Id}

[1510] {Reault-Code}

[1511] {Experimental-Result}

[1512] {Origin-Host} ;Address of BSF

[1513] {Origin-Realm} ;Realm of BSF

[1514] {User-Name} ;IMPI

[1515] {ME-Key-Material} ;Required

[1516] {UICC-Key-Material} ;Conditional

[1517] {Key-ExpiryTime} ;Time of expicy

[1518] {BootstrapInfoCreationTime} ;Bootatrapinfo creation time

[1519] {GBA-UserSecSettings} ;Selected USSs

[1520] *{AVP}

[1521] *{Proxy-Info}

[1522] *{Route-Record}

[1523] 根据它的配置，BSF 可以或者可以不发送用户 - 名 AVP(IMPI)。

[1524] 带有 ME(Ks_NAF 或者 Ks_ext_NAF) 的强制普通密钥资料在 ME- 密钥 - 资料 AVP 中发送。仅当来自于 HSS 的 bsfInfo 中的“uicc 类型”标签被设置为“GBA_U”时，带有 UICC(Ks_int_NAF) 的普通密钥资料才在 UICC- 密钥 - 资料 AVP 中发送。

[1525] 根据它的配置，密钥 - 到期时间 AVP 包含 BSF 中的引导信息的到期时间。根据以自从 1900 年 1 月 1 日 0 起 UTC 已经经过的秒的直径时间数据格式表示到期时间。如果特殊的密钥生存期值在引导过程中的来自于 HSS 的 bsfInfo 内的“生存时间”标签中给出，当计算到期时间时，则它被使用以代替 BSF 默认配置值。

[1526] BootstrapInfoCreationTime AVP 包含 bootstrapinfo 创建时间，即，BSF 中的引导信息创建时间。Bootstrapinfo 创建时间以自从 1900 年 1 月 1 日 00:00:00.000 UTC 已经经过的秒表示。

[1527] BSF 根据请求消息中的 GBA- 服务 - 标识符从引导信息中存储的 GAA-UserSecSettings 选择针对 GBA-UserSecSettings AVP 的适当的用户安全设置（如果有的话）。

[1528] 当接收到 BIA 时，NAF 中的过程描述于 3GPP TS 33.220[5]、3GPPTS 33.222[11] 并且可选择在 GAA 服务类型特定 TS 中。

[1529] 6 用于 Zh 和 Zn 接口的直径协议

[1530] 6.1 命令码值

[1531] Zn 接口分配新的命令 - 码 310。

[1532] Zn 接口中的消息使用与 3GPP TS 29.229[3] 中定义的用于 Cx 接口的多媒体 -Auth- 请求 / 应答消息相同的命令 - 码值 303。

[1533] 6.2 结果码 AVP 值

[1534] 本节定义了由所有符合本规范的直径实现肯定支持的新的结果码值。当在此定义的结果码值的一个包括于相应中时，它应该在实验性 - 结构 AVP 内部并且结果 - 码 AVP 应

该不存在。

[1535] 6.2.1 成功

[1536] 落在成功类别内的错误被用于通知同等实体已经成功完成请求。

[1537] 在 3GPP TS 29.229[3] 中定义的用于 Cx 接口的成功类别结果码是无用的并且因此在 Zh 和 Zn 接口中不需要。

[1538] 6.2.2 永久性失败

[1539] 落在永久性失败类别内的错误被用于通知同等实体请求失败，并且不应该再次尝试。

[1540] 在 3GPP TS 29.229[3] 中定义的用于 Cx 接口的永久性失败类别结果码是无用的并且因此在 Zh 和 Zn 接口中不需要。

[1541] 6.2.2.1 DIAMETER_ERROR_IMPI_UNKNOWN(5401)

[1542] 对于未知的 IMPI，由 HSS 接收到的消息。

[1543] 6.2.2.2 DIAMETER_ERROR_NOT_AUTHORIZED(5402)

[1544] 由 BSF 接收的 BSF 不能授权的消息。在此情况中，NAF 应该向 UE 指示服务不被允许。

[1545] 6.2.2.3

[1546] DIAMETER_ERROR_TRANSACTION_IDENTIFIER_INVALID(5403)

[1547] 对于无效（例如未知或到期）的引导事务标识符 (B-TID) 由 BSF 接收的消息。在此情况中，NAF 应该向 UE 请求再次引导。

[1548] 6.2.2.4 空

[1549] 6.2.2.5 空

[1550] 6.2.2.6 空

[1551] 6.2.2.7 空

[1552] 6.3 AVP

[1553] 在 3GPP TS 29.229[3] 中定义的用于 3GPP IMS Cx 接口多媒体 -Auth- 请求 / 应答消息的 AVP 如其所是地使用。

[1554] 下列表格描述了用于 Zh 和 Zn 接口协议、它们的 AVP 码值、类型、可能标记值和 AVP 是否可以被加密定义的额外的新的直径 AVP。所有定义与本规范中的 AVP 的提供商 -Id 头应该被设置为 3GPP(10415)。

[1555] 表 6.1 新的直径多媒体应用 AVP

[1556]

					AVP 标记规则			
	属性名称	AVP 码	定义的章节	值的类型	必须	可以	不应该	必须不	可以加密
	GBA-UserSecSettings	400	6.3.1.1	OctedString	M, V				否
	事务-标识符	401	6.3.1.2	OctetString	M, V				否
	NAF-主机名	402	6.3.1.3	OctetString	M, V				否
	GAA-服务-标识符	403	6.3.1.4	OctedString	M, V				否
	密钥-到期时间	404	6.3.1.5	时间	M, V				否
	ME-密钥-资料	405	6.3.1.	OctedString	M,				否

[1557]

			6		V				否
UICC-密钥-资料	406		6.3.1.7	OctedString	M,V				否
GBA U-察觉-指示符	407		6.3.1.8	枚举	M,V				否
BootstrapInfoCreationTime	408		6.3.1.9	时间	M,V				否
GUSS-时间戳	409		6.3.1.10	时间	V			M	否
注意1：‘M’表示的AVP头比特指示是否需要AVP支持。‘M’表示的AVP头比特指示可选的提供商-ID域是否存在于AVP头中。									

[1558] 6.3.1 公共 AVP

[1559] 6.3.1.1 GBA-UserSecSettings AVP

[1560] GBA-UserSecSettings AVP(AVP 码 400) 是 OctetString 类型。如果在 Zh 接口上传输，它包含 GBA 用户安全设置 (GUSS)。如果在 Zn 接口上传输，它仅包含相关 USS。GBA-UserSecSettings AVP 的内容是定义于附录 A 中的 XML 文档。

[1561] 6.3.1.2 事务 - 标识符 AVP

[1562] 事务 - 标识符 AVP(AVP 码 402) 是 OctetString 类型。此 AVP 包含引导事务标识符 (B-TID)。

[1563] 6.3.1.3 NAF- 主机名

[1564] NAF- 主机名 AVP(AVP 码 402) 是 OctetString 类型。此 AVP 包含 UE 使用的 NAF 的全资格域名 (FQDN)。可以是与 BSF 知道 NAF 的不同的域名。

[1565] 6.3.1.4 GAA- 服务 - 标识符 AVP

[1566] GAA- 服务 - 标识符 AVP(AVP 码 403) 是 OctetString 类型。此 AVP 通知 BSF 关于通过 NAF 的 GAA- 服务支持。根据此 AVP，BSF 可以选择正确的用户安全设置。

[1567] 对于 3GPP 标准化服务 (例如，PKI 端口)，GAA- 服务 - 标识符 (GSID) 应该在 0 到 999999 范围内，并且对于 GSID 的当前标准化值应该是特定服务的 GAA- 应用 - 类型 - 码。用于 3GPP 标准化服务的 GAA 服务类型码定义于附录 B 中。

[1568] 注意 ：未来，与 GAA 服务类型码不同的标准化 GSID 值可以标准化 (例如，为了在服务“MBMS 流”和“MBMS 下载”间区分)。

[1569] 例子 ：对于所有 PKI- 端口 GSID 是“1”，并且对于所有 MBMS 服务 GSID 是“4”。

[1570] 6.3.1.5 密钥 - 到期时间 AVP

[1571] 密钥 - 到期时间 AVP(AVP 码 404) 是时间类型。此 AVP 通知 NAF 关于密钥的到期时间。

[1572] 6.3.1.6 ME- 密钥 - 资料 AVP

[1573] 所要求的 ME- 密钥 - 资料 AVP(AVP 码 405) 是 OctetString 类型。NAF 正在与移动设备 (ME) 共享此密钥资料 (GBA ME 情况中的 Ks_NAF 或 GBA_U 情况中的 Ks_ext_NAF)。

[1574] 6.3.1.7 UICC- 密钥 - 资料 AVP

[1575] 条件 UICC- 密钥 - 资料 AVP(AVP 码 406) 是 OctetString 类型。NAF 可以与 UICC 中的安全元素 (例如 USIM、ISIM 等) 共享此密钥资料 (GBA_U 情况中的 Ks_int_NAF)。仅一些 GAA 应用使用此有条件的 AVP。

[1576] 6.3.1.8 GBA_U- 察觉 - 指示符

[1577] 有条件的 GBA_U- 察觉 - 指示符 AVP(AVP 码 407) 是枚举类型的。定义了下列值。

[1578] NO(0) 发送节点不是 GBA_U 察觉的

[1579] YES(0) 发送节点是 GBA_U 察觉的

[1580] 默认值是 0 即此 AVP 的缺少指示发送节点不是 GBA_U 察觉的。

[1581] 6.3.1.9 BootstrapInfoCreationTime AVP

[1582] BootstrapInfoCreationTime AVP(AVP 码 408) 是时间类型的。此 AVP 通知 NAF 关于密钥的 bootstrapinfo 创建时间。

[1583] 6.3.1.10 GUSS- 时间戳 AVP

[1584] GUSS- 时间戳 AVP(AVP 码 409) 是时间类型的。如果传输了,则此 AVP 通知 HSS 关于 BSF 中存储的 GUSS 的时间戳。

[1585] 6.4 用户身份到 HSS 的解析

[1586] 当网络运营商已经部署了多个并且可以分别寻址的 HSS 时,用户身份到 HSS 解析机制使 BSF 能够发现用于给定用户的用户数据的 HSS 的地址。在利用单个 HSS 的网络中或者当 BSF 被配置使用预定义的 HSS 时,不需要解析机制。

[1587] 解析机制是基于订阅定位符功能 (SLF) 的,并且等效于描述的用于 3GPP TS 23.228[12] 中描述的 Cx/Dx 接口。BSF 通过 Dz 接口访问订阅定位符。Dz 接口总是结合 Zh 接口一起使用。Dz 接口是基于直径。它的功能性通过由增强直径重定向代理提供的路由机制方式实现的,其能够从接收的请求中提取用户身份。

[1588] 为了得到 HSS 地址,BSF 向 SLF 发送指向 HSS 的 Zh 请求。在从 SLF 接收 HSS 地址时,BSF 应该将 Zh 请求发送到 HSS。BSF 可以存储 HSS 地址并且在与相同用户相关的进一步请求中使用它。

[1589] 在网络中,其中需要使用用户身份到 HSS 解析机制并且不配置 BSF 使用预定义的 HSS,每个 BSF 通过实现此解析机制的 SLF 的地址 / 名称来配置。

[1590] 7 名字空间 (namespace) 的使用

[1591] 本章包含已经在此 3GPP 规范中或者在 3GPP 规范 3GPP TS

[1592] 29.229[3] 中创建的,或者分配给由 IANA 管理的现存名字空间的值的名字空间。

[1593] 7.1 AVP 代码

[1594] 本规范保留 3GPP 提供商特定值 10415 :400-499 并且时间从用于 3GPP 直径应用 ([8]) 的 3GPP AVP 码名字空间中为 GAA 分配值 10415 :400-408。3GPP 提供商专用 AVP 码空间由 3GPP CN4 管理。见本规范中针对名字空间的分配的第 6 章。

[1595] 除了直径基础协议 AVP[1],此规范重用下列来自于 3GPP TS29.229[3] 的 AVP :认证 - 会话 - 状态、用户 - 名、SIP-Auth- 数据 - 条目和 SIP- 号 -Auth- 条目。

[1596] 7.2 实验性 - 结果 - 码 AVP 值

[1597] 本规范保留验性 - 结果 - 码 AVP 值 10415 :2401-2409 和 10415 :5401-5409。见 6.2 节。

[1598] 7.3 命令码值

[1599] 本规范中仅使用来自于 3GPP TS 29.229[3] 的命令 - 码 310 和 303。

[1600] 本规范仅重用命令 - 码值,而不是原规范的内容。在 TS 29.229[3] 中定义为要求但是在 Zh 或 Zn 接口中不需要的 AVP 被移除,并且因此在 Zh 或 Zn 接口消息中不要求。所有用于 GAA 的新的 AVP 被定义为可选,尽管它们在 GAA 观点中可以是强制的。

[1601] 本规范不分配新命令码给 3GPP TS 29.229[3]。

[1602] 附录 A(标准化的) :

[1603] GBA-UserSecSettings XML 定义

[1604] 本附录包含用于承载 Zh 和 Zn 接口中的 GBA-UserSecSettings AVP 内的 GBA 用户安全设置的 XML 文档的 XML 模式定义。

[1605]

```
<? xml version =" 1.0" encoding =" UTF-8" ? >
<xs:schema targetNamespace =" guss-schema-of-3gPP-gaa"
    xmlns:tns =" guss-schema-of-3gPP-gaa"
    xmlns:xs =" http://www.w3.org/2001/XMLSchema"
    elementFormDefault =" qualified"
    attributeFormDefault =" unqualified" >
 <! --This import brings in the XML language attribute xml:lang-->
 <xs:import namespace =" http://www.w3.org/XML/1998/namespace"
    schemaLocation =" http://www.w3.org/2001/xml.xsd" />
<! --The whole user's GBA specific data set -->
<xs:complexTyPe name =" guss" >
  <xs:sequence>
    <xs:element ref =" bsfInfo" minOccurs =" 0" />
    <xs:element ref =" ussList" />
    <xs:element name =" timestamp" type =" xs:dateTime"
minOccurs =" 0" />
  <xs:any processContents =" lax" minOccurs =" 0"
maxOccurs =" unbounded" />
    </xs:sequence>
    <xs:attribute name =" id"  type =" xs:string" />
  </xs:complexType>
  <! --BSF specific information element-->
  <xs:complexType name =" bsfInfo" >
    <xs:sequence>
    <xs:element name =" uiccTyPe" type =" xs:string" minOccurs =" 0"
/>
    <xs:element name =" lifeTime" type =" xs:integer" minOccurs =" 0" />
    <xs:any processContents =" lax" minOccurs =" 0"
maxOccurs =" unbounded" />
    </xs:sequence>
  </xs:complexType>
```

[1606]

```
    <! --List of all users individual User Security Settings-->
    <xs:complexTyPe name =" ussList" >
        <xs:sequence minOccurs =" 0" maxOccurs =" unbounded" >
            <xs:element ref =" uss" />
              <xs:any processContents =" lax" minOccurs =" 0"
maxOccurs =" unbounded" />
    </xs:sequence>
  </xs:complexTyPe>
  <! --User Security Setting data-->
  <xs:complexTyPe name =" uss" >
    <xs:sequence>
      <xs:element ref =" uids" />
      <xs:element ref =" flags" />
      <xs:element name =" keyChoice" type =" xs:string" minOccurs =" 0" />
      <xs:any processContents =" lax" minOccurs =" 0"
maxOccurs =" unbounded" />
    </xs:sequence>
    <xs:attribute name =" id" use =" require d" tyPe =" xs:string" />
    <xs:attribute name =" type" use =" require d" type =" xs:int" />
    <xs:attribute name =" nafGroup" use =" optional" type =" xs:string" />
  </xs:complexTyPe>
  <! --User Public Identities for authentication-->
  <xs:complexType name =" uids" >
    <xs:sequence minOccurs =" 1" maxOccurs =" unbounde d" >
    <xs:element name =" uid" type =" xs:strin g" />
    <xs:any processContents =" lax" minOccurs =" 0"
maxOccurs =" unbounded" />
    </xs:sequence>
  </xs:complexTyPe>
  <! --GAA Application type specific Authorization flag codes-->
  <xs:complexTyPe name =" flags" >
    <xs:sequence minOccurs =" 0" maxOccurs =" unbounded" >
    <xs:element name =" flag" type =" xs:int" />
    <xs:any processContents =" lax" minOccurs =" 0"
maxOccurs =" unbounded" />
    </xs:sequence>
```

[1607]

```
  </xs:complexType>
</xs:schema>
```

[1608] 注意：复合类型中的<xs：任何>元素允许未来版本中的兼容扩展。该值是：

[1609] ●元素“guss”中的属性“id”的值与用户－名 AVP 中使用的用户的 IM 私有身份

(IMPI) 相同。

[1610] ●元素“guss”中的元素“时间戳”的值与 GUSS- 时间戳 AVP 中使用的 GUSS- 时间戳是相同类型并且指示 GUSS 的时间戳。时间戳值应该以 UTC 形式表示，由紧跟着该值的时间部分的时区指示符“Z”指示。

[1611] ●元素“guss”中的属性“id”的值与 GAA- 服务 - 标识符 AVP 中使用的服务标识符 (GSID) 相同。

[1612] ●元素“bsfInfo”中的元素“uicc 类型”的值是：

[1613] GBA，以指示基本情况，或者

[1614] GBA_U，以指示 BSF 中也要求 Ks_int_NAF 的生成。

[1615] 默认值是 GBA。

[1616] ●元素“bsfInfo”中的元素“生存时间”的值只是用户特定密钥生存时间（以秒计的持续时间）。如果缺少生存时间元素，则在 BSF 中使用默认值。

[1617] ●元素“uss”中的属性“类型”的值是附录 B 中定义的 GAA 服务类型码。

[1618] ●元素“uss”中的属性“nafGroup”的值是用于 USS 是有效的 NAF 组的运营商内部组指示符。如果缺少此属性，那么仅属性“id”用于此元素的选择。

[1619] ●元素“uid”的值是来自于 HSS 的用户的公有认证身份。

[1620] ●元素“标记”的值是用于父母 uss 元素中的类型属性中指示的 GAA 服务类型来自 HSS 的用户授权标记码。如果授权标记存在，则 NAF 具有给出相应服务的许可，否则没有。

[1621] ●元素“uss”中的元素“密钥选择”的值是“ME-based- 密钥”，即，应该使用 Ks_NAF 或 Ks_ext_NAF，或者“UICC-based- 密钥”，

[1622] 即应该使用 Ks_int_NAF 或者“ME-UICC-based- 密钥”，即，可以使用 Ks_ext_NAF 或 Ks_int_NAF。此属性的值向 NAF 指示应该使用哪个密钥。如果缺少密钥选择属性，那么 NAF 应该使用默认的“ME-based- 密钥”.

[1623] 在下列说明性例子中，值是斜体的和下划线的。一个用户安全设置的内容被框起来。

[1624] <guss id =" 358500004836551@ims.mnc050.mcc358.3gppnetwork.org" >

[1625] <bsfInfo>

[1626] <lifeTime>86400</lifeTime>

[1627] </bsfInfo>

[1628] <ussList>

[1629]

```
<USS id=" 1" type=" 1" >
    <uids>
       <uid>tel:358504836551</uid>
       <uid>lauri.laitinen@nokia.com</uid> ...
  </uids>
  <flags>
      <flag>1</flag>...
   </flnags>
</uss>
```

[1630] </ussList>

[1631] </guss>

[1632] 上面用于用户“358500004836551@ims.mnc050.mcc358.3gppnetwork.org”的 GAA 用户安全设置的例子定义了对于 PKI- 端口 (GAA 服务类型码是 1) 服务被允许用于用户身份“tel :358504836551”和 lauri.laitinen@nokia.com，并且允许认证 (存在标记 1) 但是对于提供由“1”GAA 服务标识符标识的 GAA 服务的 NAF 反拒认不被允许 (缺少标记 2)。BSF 将不生成 UICC-Ks，因为 uicc 类型缺少。特定的密钥生存期定义了在其之后密钥到期的 athe 持续时间是 86400 秒，。

[1633] 附录 B(标准化的) :GAA 服务类型码

[1634] GAA 服务类型码值被用在 GAA 中以指示阐明、编码和 GAA 服务类型特定数据的使用。

[1635] 例如，每个 GAA 服务类型可以拥有它们自己的授权标记集合。这些标记的含义和译码在附录 C 中定义。随着未来它们自己的定义，也可以存在专用的 GAA 服务类型。

[1636] 码值 0-999999 是为标准化 GAA 服务类型保留的。

[1637] 定义下列值用于随 3GPP 规范的标准化 GAA 服务类型 :

[1638] 0 非特定服务

[1639] 1 PKI- 端口

[1640] 2 认证代理

[1641] 3 在线

[1642] 4 MBMS

[1643] 默认值是 0。非特定服务可以或可以不具有包含或不包含公有身份列表的用户安全设置。非特定服务不能具有特定的授权标记或者其他服务类型特定数据。

[1644] 附录 C(标准化的) :GAA 授权标记码

[1645] 对于具有定义特殊授权标记码的集合的 GAA 服务，保持下列原则 :仅当用户的用户安全设置保护那个标记的时候，由 GAA 授权标记码指定的服务被允许用于用户。

[1646] 在之前附录 B 中列出的下列标准化的 GAA 服务类型具有下列特殊授权标记码 :

[1647] PKI- 端口 (1)

[1648] 1 允许认证

[1649] 2 允许反拒认

[1650] 附录 D（资料性的）：

[1651] 更改历史

[1652]

更改历史							
日期	TSG #	TSG Doc.	CR	Rev	主题 / 意见	旧	新
2004-09	CN#25	NP-040410			CN#25 中同意的版本 2.0.0	2.0.0	6.0.0
2004-12	CN#26	NP-040580	001		授权标记码附录	6.0.0	6.1.0
2004-12			002		GAA 服务标识符的最终化		
2004-12			003	1	GUSS 的 BSF 控制信息 (bsfInfo) 标记		
2004-12			005		GAA 服务标识符的结构		
2004-12			006	1	术语的最终化		
2004-12			008	1	命令码 310 Zn 消息		
			009		NAF 组的介绍		
2005-01					修整词语问题	6.1.0	6.1.1

2005-03	CN#27	NP-050041	010		GAA 错误码	6.1.1	6.2.0
			011		从 HSS 到 BSF 的仅有一个 AV		
			012		生存期 / 到期时间术语的澄清		
			013	1	到 Z- 接口应用标识符		
			014	1	密钥生存期资料的修改		
2005-06	CT#28	CP-050090	0015		XML 扩展性	6.2.0	6.3.0
			0016	1	从拜访网络移除 BSF		
2005-09	CT#29	CP-050300	0017	1	对带有多个 HSS 的 GBA 的更正	6.3.0	6.4.0
			002		TS 33.220 的密钥命名联盟		

[1653]

			1				
2005-09	CT#29	CP-050317	0019	1	USS 中的密钥指示	6.4.0	7.0.0
			0020	2	到 Zh 参考点的 GUSS 时间戳的添加		

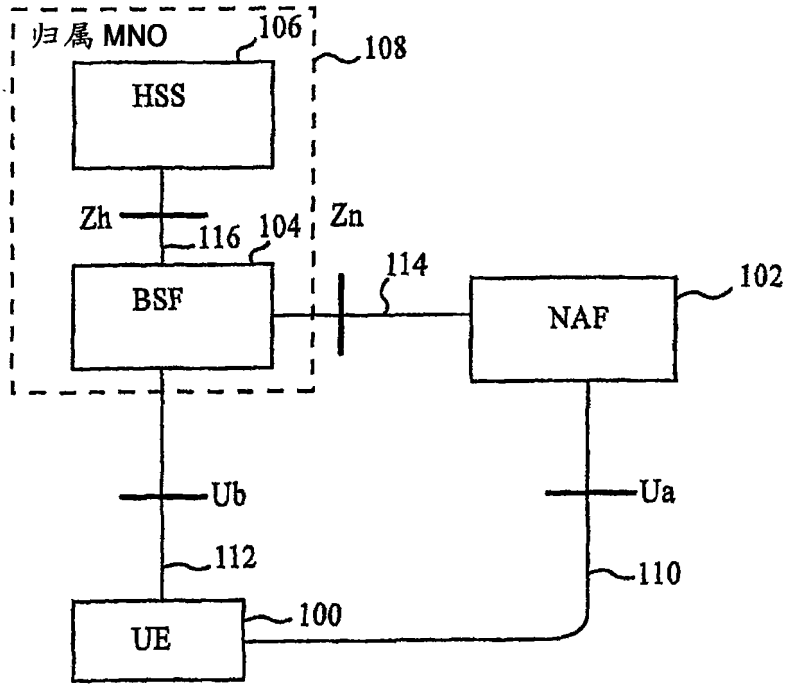

归属 MNO
106
108
HSS
Zh
116
104
Zn
114
BSF
NAF
102
Ub
Ua
112
110
UE
100

图 1

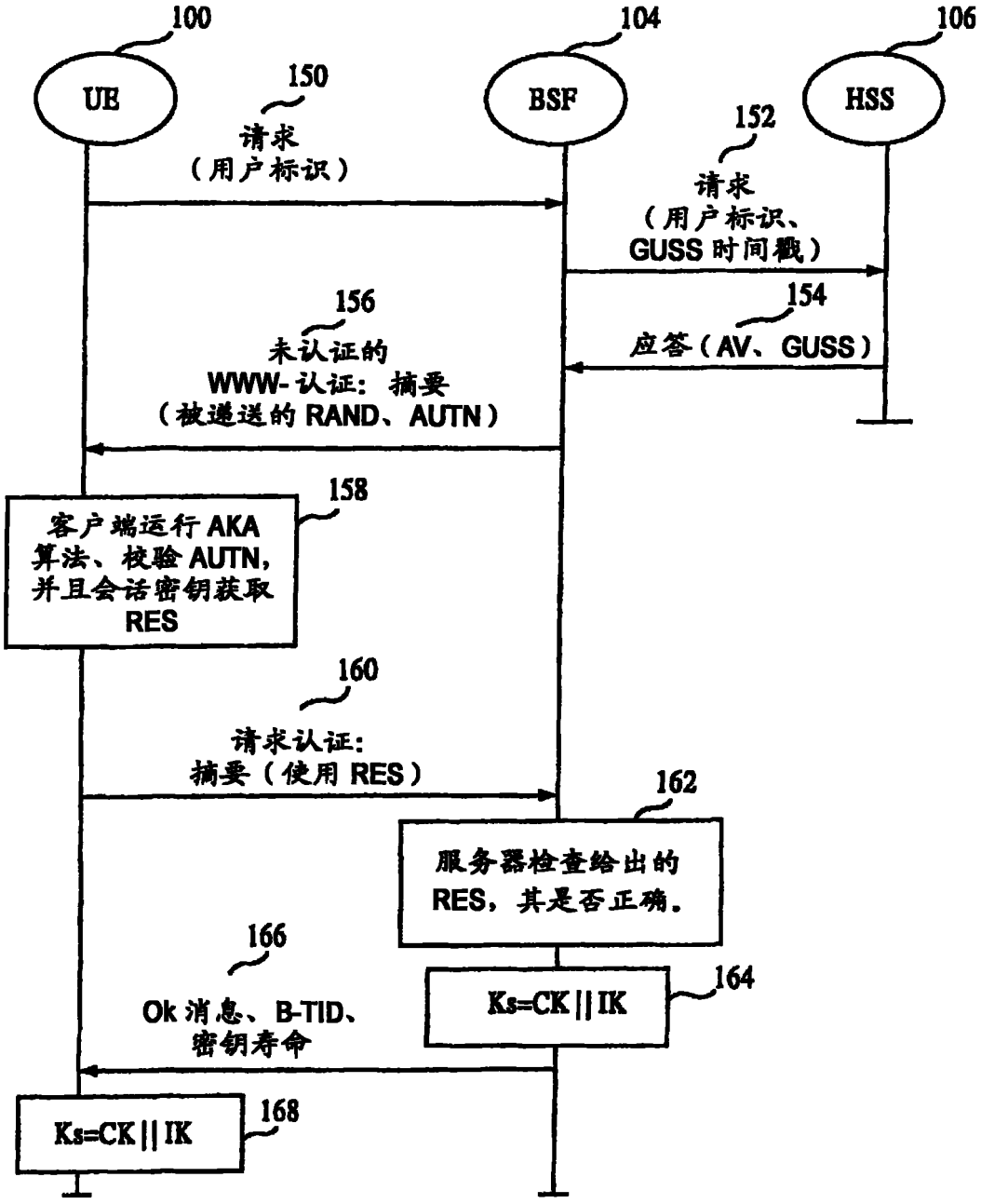

100
UE
104
BSF
106
HSS
150
请求
（用户标识）
152
请求
（用户标识、
GUSS 时间戳）
154
应答（AV、GUSS）
156
未认证的
WWW-认证：摘要
（被递送的 RAND、AUTN）
158
客户端运行 AKA
算法、校验 AUTN，
并且会话密钥获取
RES
160
请求认证：
摘要（使用 RES）
162
服务器检查给出的
RES，其是否正确。
164
Ks=CK||IK
166
Ok 消息、B-TID、
密钥寿命
168
Ks=CK||IK

图 2

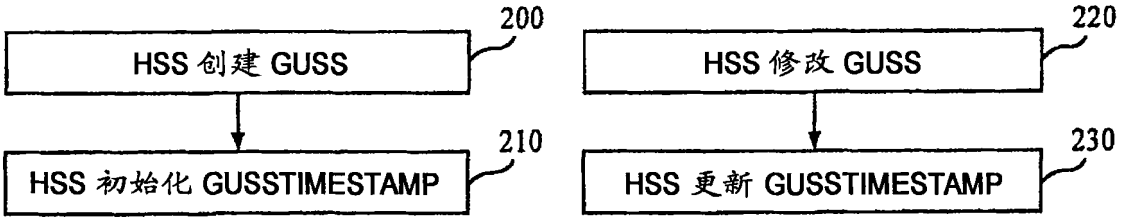

200
HSS 创建 GUSS
210
HSS 初始化 GUSSTIMESTAMP
220
HSS 修改 GUSS
230
HSS 更新 GUSSTIMESTAMP

图 3A

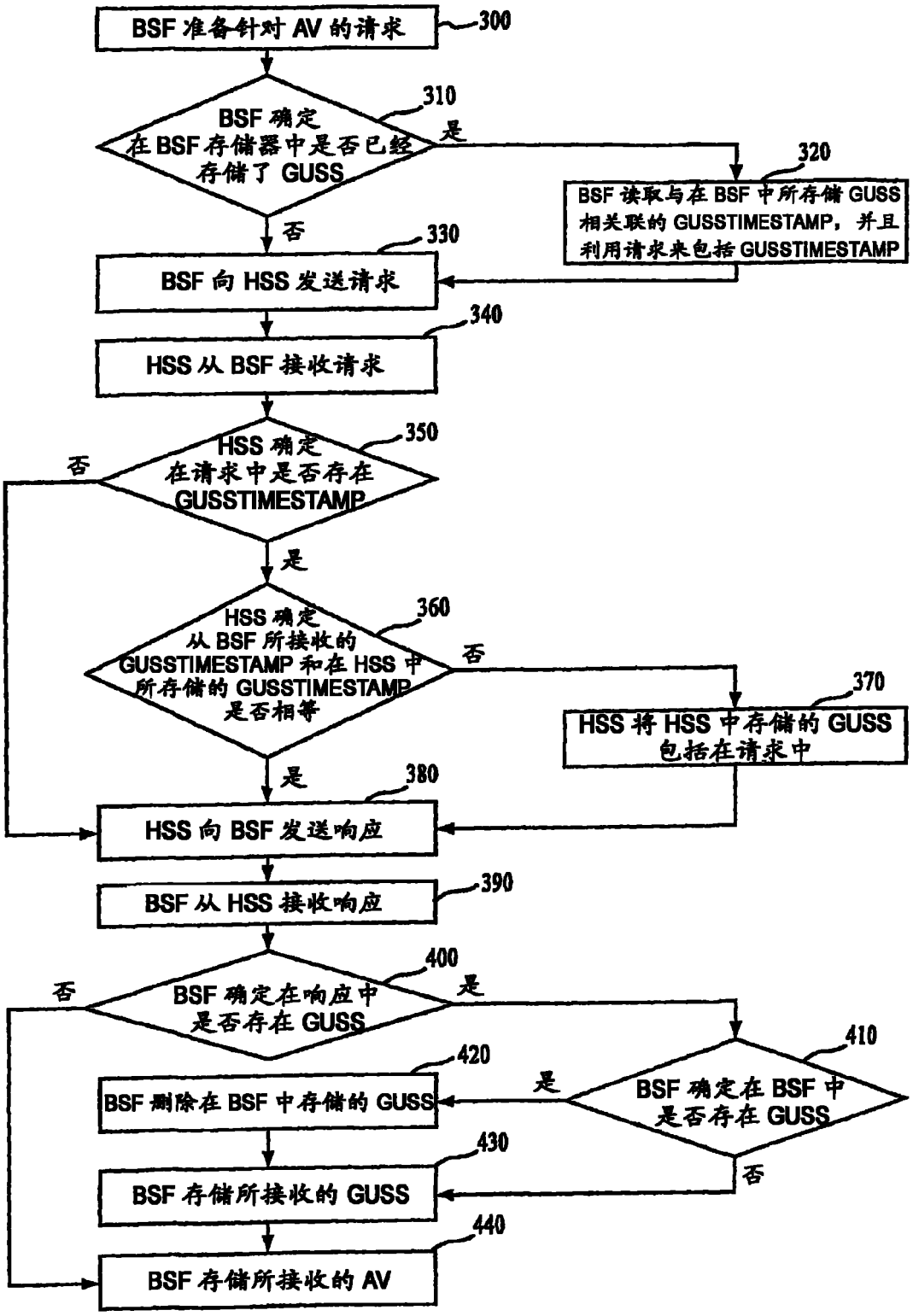

BSF 准备针对 AV 的请求
300
BSF 确定在 BSF 存储器中是否已经存储了 GUSS
310
是
否
BSF 读取与在 BSF 中所存储 GUSS 相关联的 GUSSTIMESTAMP，并且利用请求来包括 GUSSTIMESTAMP
320
BSF 向 HSS 发送请求
330
HSS 从 BSF 接收请求
340
HSS 确定在请求中是否存在 GUSSTIMESTAMP
350
否
是
HSS 确定从 BSF 所接收的 GUSSTIMESTAMP 和在 HSS 中所存储的 GUSSTIMESTAMP 是否相等
360
否
HSS 将 HSS 中存储的 GUSS 包括在请求中
370
是
HSS 向 BSF 发送响应
380
BSF 从 HSS 接收响应
390
BSF 确定在响应中是否存在 GUSS
400
否
是
BSF 确定在 BSF 中是否存在 GUSS
410
是
BSF 删除在 BSF 中存储的 GUSS
420
否
BSF 存储所接收的 GUSS
430
BSF 存储所接收的 AV
440

图 3B