(19)中华人民共和国国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 101800981 A
(43)申请公布日 2010.08.11

(21)申请号 201010104374.X

(22)申请日 2010.01.25

(71)申请人 上海华为技术有限公司
地址 200121 上海市浦东新区宁桥路615号

(72)发明人 宋照红 李瀛

(74)专利代理机构 深圳市深佳知识产权代理事务所(普通合伙) 44285
代理人 彭愿洁 李文红

(51)Int.Cl.
H04W 12/04(2009.01)
H04W 12/06(2009.01)
H04W 12/08(2009.01)

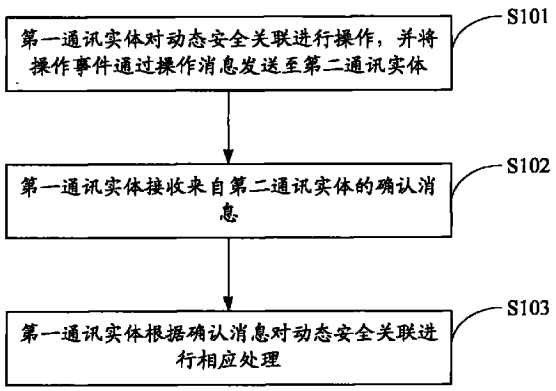
权利要求书 3 页 说明书 13 页 附图 5 页

(54)发明名称

动态安全关联的管理方法及一种通讯实体

(57)摘要

本发明实施例提供动态安全关联的管理方法及一种通讯实体，旨在解决现有技术中通讯实体对动态安全关联的支持能力不能通过协商获取以及对动态安全关联进行管理需通过和其他流程配合完成的问题。所述方法包括：第一通讯实体对动态安全关联进行操作，并将操作事件通过操作消息发送至第二通讯实体；所述第一通讯实体接收来自第二通讯实体的确认消息；所述第一通讯实体根据所述确认消息对所述动态安全关联进行相应处理。基于本发明，第一通讯实体和第二通讯实体可以获知彼此的能力，建立良好的配合，从而使用DSA更好地对业务流进行保护。



CN 101800981 A

1. 一种动态安全关联的管理方法，其特征在于，包括：

第一通讯实体对动态安全关联进行操作，并将操作事件通过操作消息发送至第二通讯实体；

所述第一通讯实体接收来自第二通讯实体的确认消息；

所述第一通讯实体根据所述确认消息对所述动态安全关联进行相应处理。

2. 如权利要求 1 所述的方法，其特征在于，若所述操作事件为创建动态安全关联且确认消息表示接受所述创建的动态安全关联，则所述第一通讯实体根据所述确认消息对所述动态安全关联进行相应处理包括：

所述第一通讯实体向所述第二通讯实体发送数据的加密 / 解密密钥。

3. 如权利要求 1 所述的方法，其特征在于，所述操作事件为修改动态安全关联时，所述第一通讯实体向所述第二通讯实体发送的操作消息至少包括帧号，所述帧号用于指明第一通讯实体和第二通讯实体将于所述帧号表示的帧的到达时刻将原动态安全关联更新为修改之后的动态安全关联。

4. 如权利要求 3 所述的方法，其特征在于，若所述确认消息表示接受所述修改后的动态安全关联，则所述第一通讯实体根据所述确认消息对所述动态安全关联进行相应处理包括：

第一通讯实体在所述帧号表示的帧的到达时刻启用修改后的动态安全关联。

5. 如权利要求 1 所述的方法，其特征在于，所述操作事件为删除所述动态安全关联时，所述第一通讯实体对动态安全关联进行操作，并将所述操作事件通过操作消息发送至第二通讯实体包括：

第一通讯实体向所述第二通讯实体发送用于删除所述动态安全关联的删除消息，同时禁用所述被删除的动态安全关联中业务流加密密钥的加密功能并保持解密功能，所述删除消息至少包括将被删除的动态安全关联的标识。

6. 如权利要求 5 所述的方法，其特征在于，所述第一通讯实体根据所述确认消息对所述动态安全关联进行相应处理包括：

若所述确认消息表示接受删除所述动态安全关联，则所述第一通讯实体禁用所述被删除的动态安全关联中的业务流加密密钥的解密功能并释放所述业务流加密密钥状态机。

7. 如权利要求 1 至 6 任意一项所述的方法，其特征在于，所述第一通讯实体对动态安全关联进行操作，并将所述操作事件通过操作消息发送至第二通讯实体后，所述方法进一步包括：

第一通讯实体等待所述第二通讯实体对所述操作消息的确认消息，若等待时间超过设定的时间，则所述第一通讯实体重复向第二通讯实体发送所述操作消息。

8. 如权利要求 1 所述的方法，其特征在于，所述第一通讯实体为基站，第二通讯实体为用户终端。

9. 一种通讯实体，其特征在于，包括：

操作模块，用于对动态安全关联进行操作，并将操作事件通过操作消息发送至第二通讯实体；

接收模块，用于接收来自所述第二通讯实体的确认消息；

处理模块，用于根据所述确认消息对所述动态安全关联进行相应处理。

10. 如权利要求 9 所述的基站，其特征在于，所述操作模块包括：

创建单元，用于创建动态安全关联并将所述创建事件通过操作消息发送至所述用户终端；或

修改单元，用于修改动态安全关联并将所述修改事件通过操作消息发送至所述用户终端；或

删除单元，用于删除动态安全关联并将所述修改事件通过操作消息发送至所述用户终端。

11. 一种动态安全关联的管理方法，其特征在于，包括：

第二通讯实体接收第一通讯实体发送的用于与所述第二通讯实体协商操作动态安全关联的协商消息；

所述第二通讯实体根据所述协商消息和自身能力参数对所述动态安全关联进行操作，并向所述第一通讯实体发送响应消息；

所述第二通讯实体接收来自所述第一通讯实体针对所述响应消息所发送的确认消息，若所述确认消息表示所述第一通讯实体接受所述第二通讯实体对所述动态安全关联的操作，则所述第二通讯实体根据所述确认消息对所述动态安全关联进行相应处理。

12. 如权利要求 11 所述的方法，其特征在于，所述第二通讯实体接收的协商消息为与所述第二通讯实体协商创建动态安全关联时，所述第二通讯实体根据所述请求消息和自身能力参数对所述动态安全关联进行操作，并向所述第一通讯实体发送响应消息包括：

所述第二通讯实体创建所述动态安全关联；

所述第二通讯实体向所述第一通讯实体发送响应消息并等待所述第一通讯实体的确认消息；

所述第二通讯实体对所述动态安全关联进行相应处理包括：

所述第二通讯实体启用所述创建的动态安全关联的相关属性。

13. 如权利要求 11 所述的方法，其特征在于，若所述第二通讯实体接收的请求消息为与所述第二通讯实体协商修改动态安全关联，所述第二通讯实体根据所述请求消息和自身能力参数对所述动态安全关联进行操作，并向所述第一通讯实体发送响应消息包括：

所述第二通讯实体修改所述动态安全关联的相关属性；

所述第二通讯实体向所述第一通讯实体发送响应消息并等待所述第一通讯实体的确认消息；

所述第二通讯实体对动态安全关联进行相应处理包括：

所述第二通讯实体启用所述修改之后的动态安全关联的相关属性。

14. 如权利要求 13 所述的方法，其特征在于，所述确认消息携带帧号，所述帧号用于通知所述第二通讯实体：在所述帧号表示的帧到达之后或达到之时，所述第一通讯实体将启用所述修改之后的动态安全关联的相关属性。

15. 如权利要求 11 所述的方法，其特征在于，所述第二通讯实体接收的请求消息为与所述第二通讯实体协商删除动态安全关联时，所述第二通讯实体根据所述请求消息和自身能力参数对所述动态安全关联进行操作，并向所述第一通讯实体发送响应消息包括：

所述第二通讯实体停止使用所述即将被删除的动态安全关联对数据进行加密；

所述第二通讯实体向所述第一通讯实体发送响应消息并等待所述第一通讯实体的确

认消息；

所述第二通讯实体对动态安全关联进行相应处理包括：

所述第二通讯实体删除所述动态安全关联。

16. 如权利要求 11 至 15 任意一项所述的方法，其特征在于，若等待所述第一通讯实体的确认消息的时间超过设定时间，则第二通讯实体再次向所述第一通讯实体发送所述响应消息。

17. 如权利要求 11 所述的方法，其特征在于，所述第一通讯实体为基站，所述第二通讯实体为用户终端。

18. 一种通讯实体，其特征在于，包括：

接收模块，用于接收第一通讯实体发送的用于与所述通讯实体协商操作动态安全关联的协商消息；

操作模块，用于根据所述协商消息和自身能力参数操作所述动态安全关联并向所述第一通讯实体发送响应消息；

处理模块，用于接收来自所述第一通讯实体针对所述响应消息所发送的确认消息，在所述确认消息表示所述基站接受所述通讯实体对所述动态安全关联的操作时，根据所述确认消息对所述操作之后的动态安全关联进行相应处理。

动态安全关联的管理方法及一种通讯实体

技术领域

[0001] 本发明涉及无线接入网领域，具体涉及动态安全关联的管理方法及一种通讯实体。

背景技术

[0002] 安全关联 (Security Association，SA) 是通讯实体，例如基站 (Base Station，BS) 和用户站 (Subscriber Station，SS) 之间共享的一系列安全信息参数集，用于确保通讯实体之间的通信安全，安全关联内容包括SA标识 (SecurityAssociation IDentifier，SAID)、安全关联类型 (Security Association Type，SAT)、加密套件 (Cryptographic Suite，CS) 和业务流加密密钥参数 (TrafficEncryption Key Parameter，TEKP) 等等，其中，TEKP包括业务流加密密钥 (Traffic Encryption Key，TEK)、TEK 生命周期、TEK 序列号和初始化向量等等。数据业务在进行加密或者鉴权过程中，使用 TEK 来进行数据加密和鉴权。为了实现 TEK 的长期维护更新和业务的连续性，通常由一个 SA 管理两个 TEK 及其属性。

[0003] 在 SA 定义的基本 SA、静态 SA 和动态 SA 这三种关联类型中，动态安全关联 (Dynamic Security Association，DSA) 是一种比较灵活的安全关联技术，其与动态业务流相联系。在建立动态业务流之前，通过创建一个 DSA 就可以更好地对业务流进行保护。动态安全关联也可以在空闲的时候创建或消除，以初始化或终止特殊的业务流。因此，与主要安全关联 (Primary Security Association，PSA) 和静态安全关联 (Static Security Association，SSA) 这两种类型的安全关联相比，DSA 更加受到业界的关注。

[0004] 然而，现有的全球微波接入互通 (Worldwide Interoperability of MicrowaveAccess，WiMAX) 技术方案只定义了 DSA 的创建流程；IEEE802.16e 协议中，DSA 的支持能力也不能通过协商获取，只能在厂家对其生产的通讯实体投入实用之前通过对接测试或通过 WiMAX 论坛的约束来规定通讯实体是否支持 DSA。如此，功能支持能力不同的通讯实体之间的配合将出现问题，例如，对于旧有的用户站或未经过对接测试的用户站，基站在功能配合使用上将会无法兼容。按照现有的 WiMAX 技术方案，即使创建了一个 DSA，通讯实体也无法获知是否创建成功，或者，在创建一个新的 DSA 后却没有相应的删除、修改旧有 DSA 等流程。因此，无论是创建新的 DSA 还是释放旧有的安全关联都需要通过和其他流程配合完成。

发明内容

[0005] 本发明实施例提供动态安全关联的管理方法及一种通讯实体，旨在解决现有技术中通讯实体对动态安全关联的支持能力不能通过协商获取以及对动态安全关联进行管理需通过和其他流程配合完成的问题。

[0006] 一种动态安全关联的管理方法，包括：第一通讯实体对动态安全关联进行操作，并将操作事件通过操作消息发送至第二通讯实体；所述第一通讯实体接收来自第二通讯实体的确认消息；所述第一通讯实体根据所述确认消息对所述动态安全关联进行相应处理。

[0007] 一种通讯实体，包括：操作模块，用于对动态安全关联进行操作，并将操作事件通过操作消息发送至第二通讯实体；接收模块，用于接收来自所述第二通讯实体的确认消息；处理模块，用于根据所述确认消息对所述动态安全关联进行相应处理。

[0008] 一种动态安全关联的管理方法，包括：第二通讯实体接收第一通讯实体发送的用于与所述第二通讯实体协商操作动态安全关联的协商消息；所述第二通讯实体根据所述协商消息和自身能力参数对所述动态安全关联进行操作，并向所述第一通讯实体发送响应消息；所述第二通讯实体接收来自所述第一通讯实体针对所述响应消息所发送的确认消息，若所述确认消息表示所述第一通讯实体接受所述第二通讯实体对所述动态安全关联的操作，则所述第二通讯实体根据所述确认消息对所述动态安全关联进行相应处理。

[0009] 一种通讯实体，包括：接收模块，用于接收第一通讯实体发送的用于与所述通讯实体协商操作动态安全关联的协商消息；操作模块，用于根据所述协商消息和自身能力参数操作所述动态安全关联并向所述第一通讯实体发送响应消息；处理模块，用于接收来自所述第一通讯实体针对所述响应消息所发送的确认消息，在所述确认消息表示所述基站接受所述通讯实体对所述动态安全关联的操作时，根据所述确认消息对所述操作之后的动态安全关联进行相应处理。

[0010] 本发明实施例通过第一通讯实体操作某一动态安全关联，将操作事件通过操作消息发送至第二通讯实体并接收操作消息的确认消息，第一通讯实体根据该确认消息对某一动态安全关联进行相应处理。由于本发明的技术方案使通讯实体一方（基站或用户终端）在针对某一动态安全关联 DSA 操作时，可以让通讯实体另一方及时获知操作事件并反馈相应的消息，并不需要生产厂商提前进行对接测试。基于这些操作，第一通讯实体和第二通讯实体可以获知彼此的能力，建立良好的配合，从而使用 DSA 更好地对业务流进行保护。

附图说明

[0011] 为了更清楚地说明本发明实施例或现有技术中的技术方案，下面将对实施例或现有技术描述中所需要使用的附图作简单地介绍，显而易见地，下面描述中的附图仅仅是本发明的一些实施例，对于本领域普通技术人员来讲，在不付出创造性劳动性的前提下，还可以根据这些附图获得其他的附图。

[0012] 图 1 是本发明实施例一提供的一种动态安全关联的管理方法基本流程示意图；

[0013] 图 2 是本发明实施例二提供的一种动态安全关联的管理方法基本流程示意图；

[0014] 图 3 是本发明实施例提供的创建某一 DSA 时第一通讯实体和第二通讯实体之间的交互示意图；

[0015] 图 4 是本发明实施例提供的修改某一 DSA 时第一通讯实体和第二通讯实体之间的交互示意图；

[0016] 图 5 是本发明实施例提供的删除某一 DSA 时第一通讯实体和第二通讯实体之间的交互示意图；

[0017] 图 6 是本发明实施例一提供的一种通讯实体基本逻辑结构示意图；

[0018] 图 7 是本发明实施例二提供的一种通讯实体基本逻辑结构示意图。

具体实施方式

[0019] 下面将结合本发明实施例中的附图，对本发明实施例中的技术方案进行清楚、完整地描述，显然，所描述的实施例仅仅是本发明一部分实施例，而不是全部的实施例。基于本发明中的实施例，本领域普通技术人员在没有做出创造性劳动前提下所获得的所有其他实施例，都属于本发明保护的范围。

[0020] 请参考图 1，本发明实施例一提供的一种动态安全关联的管理方法，包括：

[0021] 步骤 S101，第一通讯实体对动态安全关联进行操作，并将操作事件通过操作消息发送至第二通讯实体。

[0022] 在本实施例中，第一通讯实体（例如，基站）对 DSA 进行操作可以是创建某一 DSA、修改某一 DSA 或删除某一 DSA。第一通讯实体在完成这些操作后，将操作事件通过操作消息发送至第二通讯实体（例如，用户终端或用户站 SS）。第二通讯实体在接收到上述操作消息后，针对该操作消息发送一个确认消息，表明其是接受还是拒绝第一通讯实体对 DSA 所执行的操作。

[0023] 密钥可以在上述操作消息中作为安全关联属性的一部分下发下去，也可通过单独的消息进行传递。密钥通过单独的消息传递时，可以通过请求 / 应答或主动发送 / 回复确认的两握手流程来完成，更严密的流程可以通过请求 / 响应 / 确认的三握手流程完成。

[0024] 以第一通讯实体创建某一 DSA 为例。第一通讯实体创建某一 DSA 成功后，如果启动加密功能，则启动 TEK 状态机，在给对端实体发送加密和解密的 TEK 密钥后才可启用数据的加密解密功能。第一通讯实体向第二通讯实体发送的创建所述 DSA 的操作消息，例如 SA_Addition 消息，指明所创建 DSA 的相关属性。在本实施例中，SA_Addition 消息格式可以如下表 1 所示：

[0025] 表 1

[0026]

属性项	具体内容
Transaction ID	唯一标识创建此 DSA 握手信令过程的事务标识
Key Sequence Number	创建此 DSA 时生成的鉴权密钥序列号
(one or more)SA-Descriptor(s)	一个或多个 DSA 描述参数，每个 DSA 包括安全
	关联标识、安全关联类型、安全关联业务类型、加密套件、业务加密密钥、密钥生存时间等属性
Digest	根据摘要算法，用鉴权密钥计算出来用于用来保护消息完整性的消息摘要

[0027]

[0028] SA_Addition 消息还可以包括帧号 (Frame Number)，帧号用于指示第一通讯实体和第二通讯实体将于该帧号表示的帧的到达时刻启用新建的 DSA。如果不带帧号则表示从收到对端实体的确认消息的时刻开始使用新建的 DSA。

[0029] 以第一通讯实体修改某一 DSA 为例。第一通讯实体修改某一 DSA 之后，并不立即启用修改之后的 DSA。第一通讯实体将修改 DSA 这一操作事件通过操作消息，例如，SA_Change

消息发送至第二通讯实体。在本实施例中，SA_Change 消息可以如下表 2 所示：

[0030] 表 2

[0031]

属性项	具体内容
Transaction ID	唯一标识修改此 DSA 握手信令过程的事务标识
Old SAID	旧的安全关联标识
New SAID	新的安全关联标识（修改后的安全关联标识）
Old SA Parameter	旧的安全关联参数（即被修改的安全关联参数）
New SA Parameter	新的安全关联参数（即修改之后的安全关联参数）
Digest	根据摘要算法，用鉴权密钥计算出来用于用来保护消息完整性的消息摘要

[0032] SA_Change 消息还可以包括帧号 (Frame Number)，帧号用于指示第一通讯实体和第二通讯实体在帧号表示的帧的到达时刻，将原 DSA 更换为修改之后的 DSA，即，在该帧号表示的帧到达的时刻启用修改之后的 DSA。如果不带帧号则表示从收到对端实体的确认消息开始使用修改之后的 DSA。

[0033] 再以第一通讯实体删除某一 DSA 为例。第一通讯实体删除某一 DSA 之时或之后，将这一操作事件通过操作消息，例如，SA_Delete 消息发送至第二通讯实体。在本实施例中，SA_Delete 消息可以如下表 3 所示：

[0034] 表 3

[0035]

属性项	具体内容
Transaction ID	唯一标识删除此 DSA 握手信令过程的事务标识
SAID	被删除的 DSA 的安全标识
Digest	根据摘要算法，用鉴权密钥计算出来用于用来保护消息完整性的消息摘要

[0036] SA_Delete 消息至少包含被删除的 DSA 的标识。

[0037] 第一通讯实体向第二通讯实体发送用于删除动态安全关联的删除消息（例如，SA_Delete 消息）的同时即停止使用被删除的 DSA 中的 TEK 的加密功能并保持解密功能，直到接收到第二通讯实体发送并表示接受删除该 DSA 的确认消息才停用解密功能，释放 TEK 状态机。

[0038] SA_Delete 消息还可以包括帧号 (Frame Number)，帧号用于指明第一通讯实体和第二通讯实体将于该帧号表示的帧的到达时刻删除 DSA，即，在该帧号表示的帧开始的时刻停止使用 DSA。如果不带帧号则表示从收到对端通讯实体的确认消息的时刻开始删除动态

安全关联。

[0039] 此外，在本实施例中，第一通讯实体操作某一动态安全关联并将操作事件通过操作消息发送至第二通讯实体后，第一通讯实体等待第二通讯实体对所述操作消息的确认消息。若在等待定时器超时前收到确认消息，则停止等待定时器；若等待定时器超过设定的时间，第一通讯仍未收到第二通讯实体的确认消息，则第一通讯实体重复向第二通讯实体发送操作消息并重启等待定时器。若超过等待定时器设定的时间后仍未收到确认消息，则可以再次重发操作消息，直至重复发送的次数超过设定的次数。

[0040] 步骤 S102，第一通讯实体接收来自第二通讯实体的确认消息。

[0041] 以第一通讯实体创建某一 DSA、发送 SA_Addition 消息为例。第一通讯实体创建某一 DSA 并发送 SA_Addition 消息至第二通讯实体时，第二通讯实体根据自身的能力反馈至第一通讯实体的确认消息 SA_ACK 可以如下表 4 所示：

[0042] 表 4

[0043]

属性项	具体内容
Transaction ID	唯一标识创建此 DSA 握手信令过程的事务标识
SA ID	创建的 DSA 的安全关联标识
Conformation Code	表示确认的状态
Digest	根据摘要算法，用鉴权密钥计算出来用于用来保护消息完整性的消息摘要

[0044] 其中，Conformation Code 属性项用来指明是否接受第一通讯实体创建某一 DSA，如不接受则通过错误原因码 (ErrCode) 指明不接受的原因。

[0045] 以第一通讯实体修改某一 DSA，发送 SA_Change 消息为例。第一通讯实体修改某一 DSA 并将这一操作事件通过操作消息（例如，SA_Change 消息）发送给第二通讯实体后，第二通讯实体根据自身的能力向第一通讯实体反馈确认消息 SA_ACK，其中指明是否接受第一通讯实体修改该 DSA，如不接受则通过错误原因码 (ErrCode) 指明不接受的原因，例如，可以是 SA 标识对应的 DSA 不存在或 SA 标识对应的 DSA 正在使用而不允许修改等等。

[0046] 再以第一通讯实体删除某一 DSA，发送 SA_Delete 消息为例。第一通讯实体删除某一 DSA 之后，将这一操作事件通过操作消息（例如，SA_Delete 消息）发送至第二通讯实体。第二通讯实体根据自身的能力向第一通讯实体反馈确认消息 SA_ACK，其中指明是否接受第一通讯实体删除该 DSA，如不接受则通过错误原因码 (ErrCode) 指明不接受的原因，例如，可以是 SA 标识对应的 DSA 不存在或 SA 标识指定的 DSA 正在使用而不允许删除等等。

[0047] 步骤 S103，第一通讯实体根据确认消息对动态安全关联进行相应处理。

[0048] 以第一通讯实体创建某一 DSA，发送 SA_Addition 消息为例。如果第二通讯实体确认此次创建的 DSA，如果启动加密功能，则启动业务流加密密钥 TEK 状态机，对数据加密并将加密 / 解密密钥发送至第二通讯实体；如果第二通讯实体拒绝此次创建的 DSA，则第一通讯实体根据第二通讯实体反馈的 SA_ACK 消息中的错误原因码 (ErrCode) 进行相应处理，例

如，中断与第二通讯实体的后续交互流程。

[0049] 以第一通讯实体修改某一 DSA，发送 SA_Change 消息为例。如果第二通讯实体确认此次修改的 DSA，则第一通讯实体在收到 SA_Change 消息的确认消息后，在 SA_Change 消息指定的帧号 (Frame Number) 表示的帧的到达时刻将原 DSA 更换修改之后的 DSA，即，在所述帧号表示的帧到达时启用修改之后的 DSA ；如果启动加密功能，则启动业务流加密密钥 TEK 状态机。如果 SA_Change 消息没有携带帧号，则第一通讯实体在收到确认消息那一帧开始启用修改后的 DSA，同样第二通讯实体在发送确认消息的那一帧开始启用修改后的 DSA。

[0050] 再以第一通讯实体删除某一 DSA，发送 SA_Delete 消息为例。如果第二通讯实体接受此次 DSA 删除，在 SA_Delete 消息指定的帧号 (Frame Number) 表示的帧的到达时刻删除 DSA，即，在所述帧号表示的帧到达时业务停用要删除的 DSA ；如果启动加密功能，则同样停止删除业务流加密密钥 TEK 状态机。如果 SA_Delete 消息没有携带帧号，则第一通讯实体在收到 SA_Delete 消息的确认消息后，第一通讯实体停用所述被删除的 DSA 中的业务流加密密钥 TEK 的解密功能并释放所述业务流加密密钥 TEK 状态机。

[0051] 从上述本发明实施例一可知，本发明的技术方案使通讯实体一方在针对某一 DSA 操作时，可以让通讯实体另一方及时获知操作事件并反馈相应的消息，并不需要生产厂商提前进行对接测试。基于这些操作，第一通讯实体和第二通讯实体可以获知彼此的能力，建立良好的配合，从而使用 DSA 更好地对业务流进行保护。

[0052] 请参阅图 2，本发明实施例二提供的一种动态安全关联的管理方法基本流程示意图。在本实施例中，第二通讯实体可以为用户终端或用户站 SS，第一通讯实体可以为基站。图 2 所示实施例二主要包括 ：

[0053] 步骤 S201，第二通讯实体接收第一通讯实体发送的用于与第二通讯实体协商操作动态安全关联的协商消息 ；

[0054] 步骤 S202，第二通讯实体根据所述协商消息和自身能力参数对所述动态安全关联进行操作，并向第一通讯实体发送响应消息 ；

[0055] 步骤 S203，第二通讯实体接收来自第一通讯实体针对响应消息所发送的确认消息，若该确认消息表示第一通讯实体接受第二通讯实体对动态安全关联的操作，则第二通讯实体对动态安全关联进行相应处理。

[0056] 以下分别以创建、修改和删除某一 DSA 为例，通过图示第二通讯实体和第一通讯实体之间的交互，说明实施例二和实施例三的技术方案。

[0057] 如图 3 所示，创建某一 DSA 时第一通讯实体和第二通讯实体之间的交互示意图，包括 ：

[0058] S301，第一通讯实体发送与第二通讯实体协商创建某一动态安全关联的协商消息。例如，第一通讯实体发送 SA_Addition_Req 消息，与第二通讯实体协商创建某一 DSA，其格式可以如下表 5 所示 ：

[0059] 表 5

[0060]

属性项	具体内容
Transaction ID	唯一标识创建此 DSA 握手信令过程的事务标识

属性项	具体内容
Random	创建此 DSA 过程中新生成的随机数
Key Sequence Number	具体的鉴权密钥序列号
Key Life Time	鉴权密钥的生存时间
Security-Capabilities	安全能力，例如，支持的数据加密算法、数据鉴权算法和业务加密密钥算法列表等
Security Negotiation Parameters	安全协商参数，包括支持的协议版本、鉴权策略、消息认证模式、数据包窗口大小、流控策略和安
	全关联数目等
(one or more)SA-Descriptor(s)	安全关联描述参数，其中，每个安全关联包括安全关联标识、安全关联类型、安全关联业务类型、加密套件、业务加密密钥和密钥生存时间等属性
Digest	根据摘要算法，用鉴权密钥计算出来用于用来保护消息完整性的消息摘要

[0061]

[0062] 由于通讯实体一方的能力或状态对另一方而言都是未知的，因此，第一通讯实体和第二通讯实体首先协商即将创建的某一 DSA 的相关属性，即，在本实施例中，SA_Addition_Req 消息应该包含即将创建的某一 DSA 的相关属性。

[0063] S302，第一通讯实体等待第二通讯实体的响应消息；

[0064] 在本实施例中，第一通讯实体在发送协商消息时可以启动一等待定时器，若该等待定时器没有超时，则第一通讯实体可以一直等待请求消息的响应消息，若等待定时器超时后还没有收到所述请求消息的响应消息，则第一通讯实体可以重新发送与第二通讯实体协商创建某一动态安全关联的协商消息并再次重新启动定时器等待定时器。若超过等待定时器设定的时间后仍未收到确认消息，则可以再次重发请求消息，直到发送请求消息的次数超过设定的重复次数。

[0065] S303，第二通讯实体接收第一通讯实体发送的与第二通讯实体协商创建某一 DSA 的协商消息，根据 DSA 的相关属性和自身能力参数创建 DSA；

[0066] S304，第二通讯实体向第一通讯实体发送协商消息的响应消息；

[0067] 响应消息，例如 SA_Additon_Rsp 消息标明第一通讯实体可以接受的 DSA 相关属性，即，响应消息包含了第一通讯实体自身能力参数和即将创建的某一 DSA 的相关属性（即第二通讯实体和第一通讯实体协商即将创建的某一 DSA 的相关属性）的交集，其格式可以如下表 6 所示：

[0068] 表 6

[0069]

属性项	具体内容
Transaction ID	唯一标识创建此 DsA 握手信令过程的事务标识
Random	新生成的随机数
Key Sequence Number	具体的鉴权密钥序列号
Key Life Time	鉴权密钥的生存时间
Security Negotiation Parameters	安全协商参数，包括支持的协议版本、鉴权策略、消息认证模式、数据包窗口大小、流控策略和安全关联数目等
(one or more)SA-Descriptor(s)	安全关联描述参数，其中，每个安全关联包括安全关联标识、安全关联类型、安全关联业务类型、加密套件、业务加密密钥和密钥生存时间等属性
Digest	根据摘要算法，用鉴权密钥计算出来用于用来保护消息完整性的消息摘要

[0070]

[0071] S305，第二通讯实体等待第一通讯实体的确认消息；

[0072] 在本实施例中，第二通讯实体在发送针对协商消息的响应消息后可以启动一等待定时器，在该等待定时器超时前，第二通讯实体可以一直等待第一通讯实体的确认消息，例如，SA_Addition_ACK 消息；若等待定时器超时后还没有收到第一通讯实体的确认消息，则第二通讯实体重新发送响应消息并重新启动等待定时器。若超过等待定时器设定的时间后仍未收到确认消息，则可以再次重发响应消息，直到发送响应消息的次数超过设定的重复次数。

[0073] S306，第一通讯实体向第二通讯实体发送对响应消息的确认消息，该确认消息标明第一通讯实体是否接受第一通讯实体创建的 DSA，若不接受，则确认消息还应该标明不接受的原因。

[0074] S307，若确认消息标明第一通讯实体接受第二通讯实体创建 DSA，则第二通讯实体启用创建的 DSA 的相关属性。

[0075] 需要说明的是，在本实施例中，响应消息的确认消息可以携带一帧号 (Frame Number)，以该帧号通知第二通讯实体：在该帧号表示的帧到达之后或达到之时第一通讯实体将启用操作之后的动态安全关联的相关属性。例如，SA_Addition_ACK 消息中携带帧号，则实际上是第一通讯实体通知第二通讯实体，其将在该帧号表示的帧到达第二通讯实体之后启用第二通讯实体创建的 DSA 的相关属性。如果确认消息没有携带帧号，则表明从发送 SA_Addition_ACK 消息帧起第一通讯实体立即启用第二通讯实体创建的 DSA 的相关属性。

[0076] 请参阅图 4，修改某一 DSA 时第一通讯实体和第二通讯实体之间的交互示意图，包括：

[0077] S401，第一通讯实体发送与第二通讯实体协商修改某一 DSA 的协商消息。例如，第一通讯实体发送 SA_Change_Req 消息，与第二通讯实体协商修改某一 DSA，其格式可以如下

表 7 所示：

[0078] 表 7

[0079]

属性项	具体内容
Transaction ID	唯一标识修改此 DSA 握手信令过程的事务标识
Random	修改此 DSA 过程中新生成的随机数
Key Sequence Number	具体的鉴权密钥序列号
Key Life Time	鉴权密钥的生存时间
Security-Capabilities	安全能力，例如，支持的数据加密算法、数据鉴权算法和业务加密密钥算法列表等
Security Negotiation Parameters	安全协商参数，包括支持的协议版本、鉴权策略、消息认证模式、数据包窗口大小、流控策略和安全关联数目等
(one or more)SA-Descriptor(s)	安全关联描述参数，其中，每个安全关联包括安全关联标识、安全关联类型、安全关联业务类型、加密套件、业务加密密钥和密钥生存时间等属性
Digest	根据摘要算法，用鉴权密钥计算出来用于用来保护消息完整性的消息摘要

[0080]

[0081] 由于通讯实体一方的能力或状态对另一方而言都是未知的，因此，第一通讯实体和第二通讯实体首先协商即将被修改的某一 DSA 的相关属性，即，在本实施例中，SA_Change_Req 消息应该包含所述即将被修改的某一 DSA 的相关属性。

[0082] S402，第一通讯实体等待第二通讯实体的响应消息；

[0083] 在本实施例中，第一通讯实体在发送协商消息时可以启动一等待定时器，若该等待定时器没有超时，则第一通讯实体可以一直等待第二通讯实体的响应消息，若等待定时器超时后还没有收到请求消息的响应消息，则第一通讯实体可以重新发送与第二通讯实体协商修改某一动态安全关联的协商消息，并再次启动等待定时器。若超过等待定时器设定的时间后仍未收到确认消息，则可以再次重发请求消息，直到发送请求消息的次数超过设定的重复次数。

[0084] S403，第二通讯实体接收第一通讯实体发送的与第二通讯实体协商修改某一 DSA 的协商消息，根据 DSA 的相关属性和自身能力参数修改 DSA；

[0085] S404，第二通讯实体向第一通讯实体发送响应消息；

[0086] 响应消息，例如 SA_Change_Rsp 消息标明第二通讯实体可以接受的 DSA 相关属性，即，该响应消息包含了第二通讯实体自身能力参数和即将被修改的某一 DSA 的相关属性（即第一通讯实体和第二通讯实体协商即将修改的某一 DSA 的相关属性）的交集，其格式可

以如下表 8 所示：

[0087] 表 8

[0088]

属性项	具体内容
Transaction ID	唯一标识修改此 DSA 握手信令过程的事务标识
Random	修改此 DSA 过程中新生成的随机数
Key Sequence Number	具体的鉴权密钥序列号
Key Life Time	鉴权密钥的生存时间
Security-Capabilities	安全能力，例如，支持的数据加密算法、数据鉴权算法和业务加密密钥算法列表等
Security Negotiation Parameters	安全协商参数，包括支持的协议版本、鉴权策略、消息认证模式、数据包窗口大小、流控策略和安全关联数目等
(one or more)SA-Descriptor(s)	安全关联描述参数，其中，每个安全关联包括安全关联标识、安全关联类型、安全关联业务类型、加密套件、业务加密密钥和密钥生存时间等属性
Digest	根据摘要算法，用鉴权密钥计算出来用于用来保护消息完整性的消息摘要

[0089]

[0090] S405，第二通讯实体等待第一通讯实体对响应消息的确认消息；

[0091] 在本实施例中，第二通讯实体在发送响应消息后可以启动一等待定时器，在该等待定时器超时前，第二通讯实体可以一直等待响应消息的确认消息，例如，SA_Addition_ACK 消息；若等待定时器超时后还没有收到响应消息的确认消息，则第一通讯实体重新发送请求消息的响应消息并启动等待定时器。若超过等待定时器设定的时间后仍未收到确认消息，则可以再次重发响应消息，直到发送响应消息的次数超过设定的重复次数。

[0092] S406，第一通讯实体向第二通讯实体发送确认消息，该确认消息表示第一通讯实体是否接受第二通讯实体修改的 DSA，若不接受，则确认消息还应该标明不接受的原因，错误的原因例如可以是 DSA 的 SA 标识指定的 DSA 不存在或 SA 标识指定的 DSA 正在使用而不允许修改等等。

[0093] S407，若确认消息标明第一通讯实体接受第二通讯实体修改 DSA，则第二通讯实体启用修改之后的 DSA 的相关属性。

[0094] 需要说明的是，在本实施例中，确认消息还可以携带一帧号 (FrameNumber)，以该帧号通知第二通讯实体：在该帧号表示的帧到达之后或达到之时第一通讯实体将启用操作之后的动态安全关联的相关属性。例如，SA_Change_ACK 消息中携带帧号，则实际上是第一通讯实体通知第二通讯实体，其将在该帧号表示的帧到达第二通讯实体之后启用第二通讯

实体创建的 DSA 的相关属性。如果确认消息没有携带帧号，则表明从发送 SA_Change_ACK 消息帧起第一通讯实体立即启用第二通讯实体修改过的 DSA 的相关属性。

[0095] 请参阅图 5，删除某一 DSA 时第二通讯实体和第一通讯实体之间的交互示意图，包括：

[0096] S501，第一通讯实体发送与第二通讯实体协商删除某一 DSA 的协商消息。例如，第一通讯实体发送 SA_Delete_Req 消息，与第二通讯实体协商删除某一 DSA，其格式可以如下表 9 所示：

[0097] 表 9

[0098]

属性项	具体内容
Transaction ID	唯一标识删除此 DSA 握手信令过程的事务标识
SAID	被删除的 DSA 的安全标识
Digest	根据摘要算法，用鉴权密钥计算出来用于用来保护消息完整性的消息摘要 .

[0099] 由于通讯实体一方的能力或状态对另一方而言都是未知的，因此，第一通讯实体和第二通讯实体首先协商即将被删除的某一 DSA，即，在本实施例中，SA_Delete_Req 消息应该包含即将被删除的某一 DSA。

[0100] S502，第一通讯实体等待第二通讯实体的响应消息；

[0101] 在本实施例中，第一通讯实体在发送协商消息时可以启动一等待定时器，若该等待定时器没有超时，则第一通讯实体可以一直等待第二通讯实体的响应消息；若改等待定时器超时后还没有收到第二通讯实体的响应消息，则第一通讯实体可以重新发送请求第二通讯实体删除某一动态安全关联的请求消息并再次启动等待定时器。若超过等待定时器设定的时间后仍未收到响应消息，则可以再次重发请求消息，直到发送请求消息的次数超过设定的重复次数。

[0102] S503，第二通讯实体接收第一通讯实体发送的与第二通讯实体协商删除某一 DSA 的请求消息，停用即将被删除的 DSA 中的业务流加密密钥 TEK 进行数据加密；

[0103] S504，第二通讯实体向第一通讯实体发送响应消息；

[0104] 响应消息，例如 SA_Delete_Rsp 消息表示第二通讯实体是否接受删除 DSA，即，响应消息包含了第二通讯实体是否接受第一通讯实体协商删除某一 DSA 的信息，其格式可以如下表 10 所示：

[0105] 表 10

[0106]

属性项	具体内容
Transaction ID	唯一标识删除此 DSA 握手信令过程的事务标识
SAID	被删除的 DSA 的安全标识

属性项	具体内容
Digest	根据摘要算法,用鉴权密钥计算出来用于用来保护消息完整性的消息摘要

[0107] S505,第二通讯实体等待第一通讯实体的确认消息 ;

[0108] 在本实施例中,第二通讯实体在发送响应消息后可以启动一等待定时器,在该等待定时器超时前,第二通讯实体可以一直等待第二通讯实体的确认消息,例如,SA_Delete_ACK 消息 ;若该等待定时器超时后还没有收到第一通讯实体的确认消息,则第二通讯实体重新发送请求消息的响应消息并重新启动该定时器。若超过等待定时器设定的时间后仍未收到确认消息,则可以再次重发响应消息,直到发送响应消息的次数超过设定的重复次数。

[0109] S506,第一通讯实体向第二通讯实体发送确认消息,该确认消息标明第一通讯实体是否接受第二通讯实体发起的对某一 DSA 的删除,若不接受,则确认消息还应该标明不接受的原因,错误的原因例如可以是 DSA 的 SA 标识指定的 DSA 不存在或 SA 标识指定的 DSA 正在使用而不允许删除等等。

[0110] S507,若确认消息表示第一通讯实体接受第二通讯实体删除 DSA,则第二通讯实体删除该 DSA。

[0111] 从上述本发明实施例二可知,本发明的技术方案使通讯实体一方在针对某一 DSA 操作时,通过更详细的协商过程可以让通讯实体另一方及时获知操作事件并反馈相应的消息,并不需要生产厂商提前进行对接测试。基于这些操作,第一通讯实体和第二通讯实体可以获知彼此的能力,建立良好的配合,从而使用 DSA 更好地对业务流进行保护。

[0112] 请参阅图 6,本发明实施例一提供的一种通讯实体基本逻辑结构示意图。为了便于说明,仅仅示出了与本发明实施例相关的部分。该通讯实体可以是基站,其包括 :

[0113] 操作模块 601,用于对动态安全关联进行操作,并将操作事件通过操作消息发送至第二通讯实体 (例如,用户终端等),其进一步包括 :

[0114] 创建单元 6011,用于创建动态安全关联并将创建事件通过操作消息发送至所述用户终端 ;或

[0115] 修改单元 6012,用于修改动态安全关联并将修改事件通过操作消息发送至所述用户终端 ;或

[0116] 删除单元 6013,用于删除动态安全关联并将修改事件通过操作消息发送至所述用户终端。

[0117] 接收模块 602,用于接收来自第二通讯实体的确认消息 ;

[0118] 处理模块 603,用于根据接收模块 602 接收的确认消息对动态安全关联进行相应处理。

[0119] 例如,若操作模块 601 执行的操作为创建一动态安全关联且接收模块 602 接收的确认消息表示用户终端接受所述创建的动态安全关联时,处理模块 603 根据确认消息向用户终端发送数据的加密 / 解密密钥。

[0120] 再如,若操作模块 601 执行的操作为修改一动态安全关联且接收模块 602 接收的确认消息表示用户终端接受修改的动态安全关联时,处理模块 603 在帧号 (Frame Number) 表示的帧的到达时刻启用修改之后的动态安全关联。

[0121] 再如，若操作模块601执行的操作为删除一动态安全关联时，处理模块603停止使用被删除的动态安全关联中的业务流加密密钥的解密功能并释放业务流加密密钥状态机。

[0122] 请参阅图7，本发明实施例二提供的一种通讯实体基本逻辑结构示意图。为了便于说明，仅仅示出了与本发明实施例相关的部分。该通讯实体可以是用户终端，其包括：

[0123] 接收模块701，用于接收第一通讯实体发送的用于与该通讯实体协商操作动态安全关联的协商消息，第一通讯实体可以是基站等；

[0124] 操作模块702，用于根据接收模块701接收的协商消息和自身能力参数操作动态安全关联并向第一通讯实体发送响应消息；

[0125] 处理模块703，用于接收来自第一通讯实体针对响应消息所发送的确认消息，在确认消息表示第一通讯实体接受用户终端对动态安全关联的操作时，对操作之后的动态安全关联进行相应处理。

[0126] 需要说明的是，上述设备各模块/单元之间的信息交互、执行过程等内容，由于与本发明方法实施例基于同一构思，具体内容可参见本发明方法实施例中的叙述，此处不再赘述。

[0127] 从上述本发明实施例可知，本发明的技术方案使通讯实体一方（基站或用户终端）在针对某一DSA操作时，可以让通讯实体另一方及时获知操作事件并反馈相应的消息，并不需要生产厂商提前进行对接测试。基于这些操作，第一通讯实体和第二通讯实体可以获知彼此的能力，建立良好的配合，从而使用DSA更好地对业务流进行保护。本动态安全管理方法作为一种通用的动态安全关联管理方法，同样可以应用在其他的系统中的安全管理上。

[0128] 本领域普通技术人员可以理解上述实施例的各种方法中的全部或部分步骤是可以通过程序来指令相关的硬件来完成，该程序可以存储于一计算机可读存储介质中，存储介质可以包括：只读存储器（ROM，Read Only Memory）、随机存取存储器（RAM，Random Access Memory）、磁盘或光盘等。

[0129] 以上对本发明实施例所提供的动态安全关联的管理方法及一种通讯实体进行了详细介绍，本文中应用了具体个例对本发明的原理及实施方式进行了阐述，以上实施例的说明只是用于帮助理解本发明的方法及其核心思想；同时，对于本领域的一般技术人员，依据本发明的思想，在具体实施方式及应用范围上均会有改变之处，综上所述，本说明书内容不应理解为对本发明的限制。

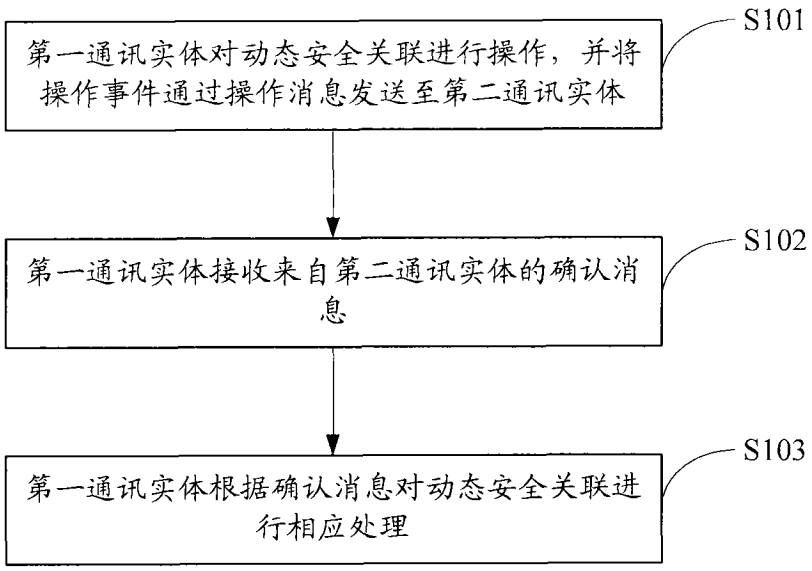

第一通讯实体对动态安全关联进行操作，并将操作事件通过操作消息发送至第二通讯实体
S101
第一通讯实体接收来自第二通讯实体的确认消息
S102
第一通讯实体根据确认消息对动态安全关联进行相应处理
S103

图 1

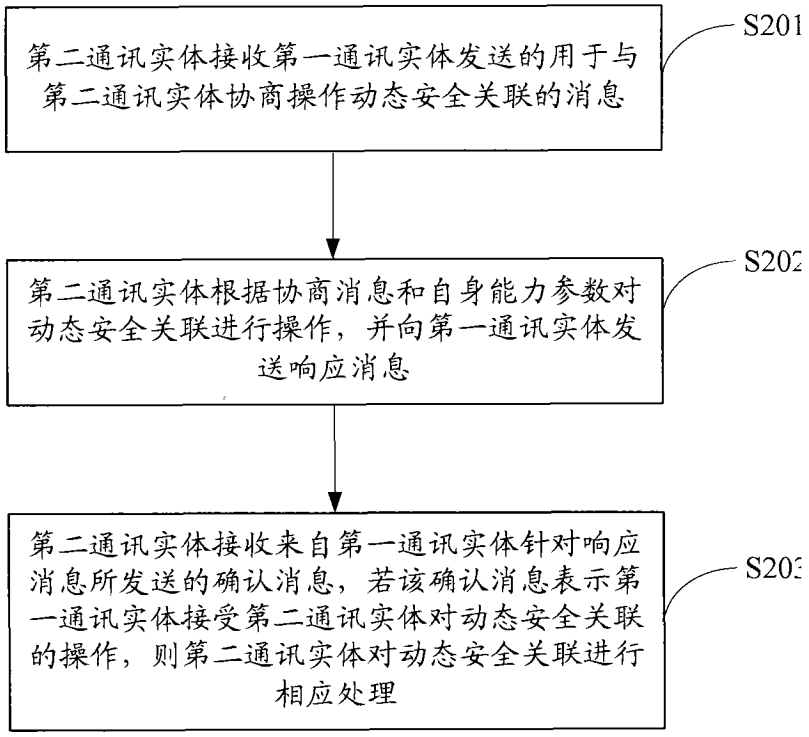

第二通讯实体接收第一通讯实体发送的用于与第二通讯实体协商操作动态安全关联的消息
S201
第二通讯实体根据协商消息和自身能力参数对动态安全关联进行操作，并向第一通讯实体发送响应消息
S202
第二通讯实体接收来自第一通讯实体针对响应消息所发送的确认消息，若该确认消息表示第一通讯实体接受第二通讯实体对动态安全关联的操作，则第二通讯实体对动态安全关联进行相应处理
S203

图 2

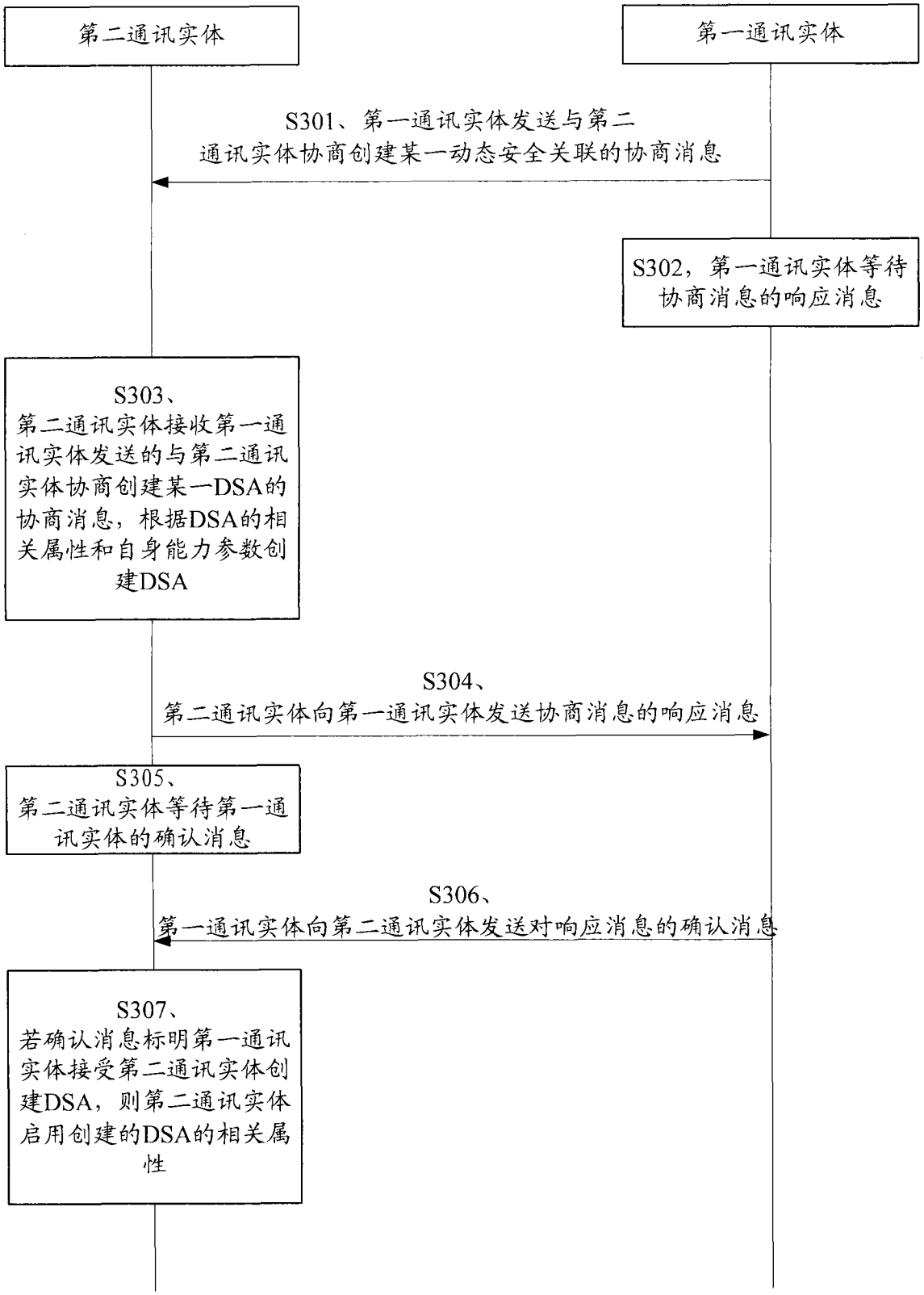

第二通讯实体
第一通讯实体
S301、第一通讯实体发送与第二通讯实体协商创建某一动态安全关联的协商消息
S302，第一通讯实体等待协商消息的响应消息
S303、第二通讯实体接收第一通讯实体发送的与第二通讯实体协商创建某一DSA的协商消息，根据DSA的相关属性和自身能力参数创建DSA
S304、第二通讯实体向第一通讯实体发送协商消息的响应消息
S305、第二通讯实体等待第一通讯实体的确认消息
S306、第一通讯实体向第二通讯实体发送对响应消息的确认消息
S307、若确认消息标明第一通讯实体接受第二通讯实体创建DSA，则第二通讯实体启用创建的DSA的相关属性

图 3

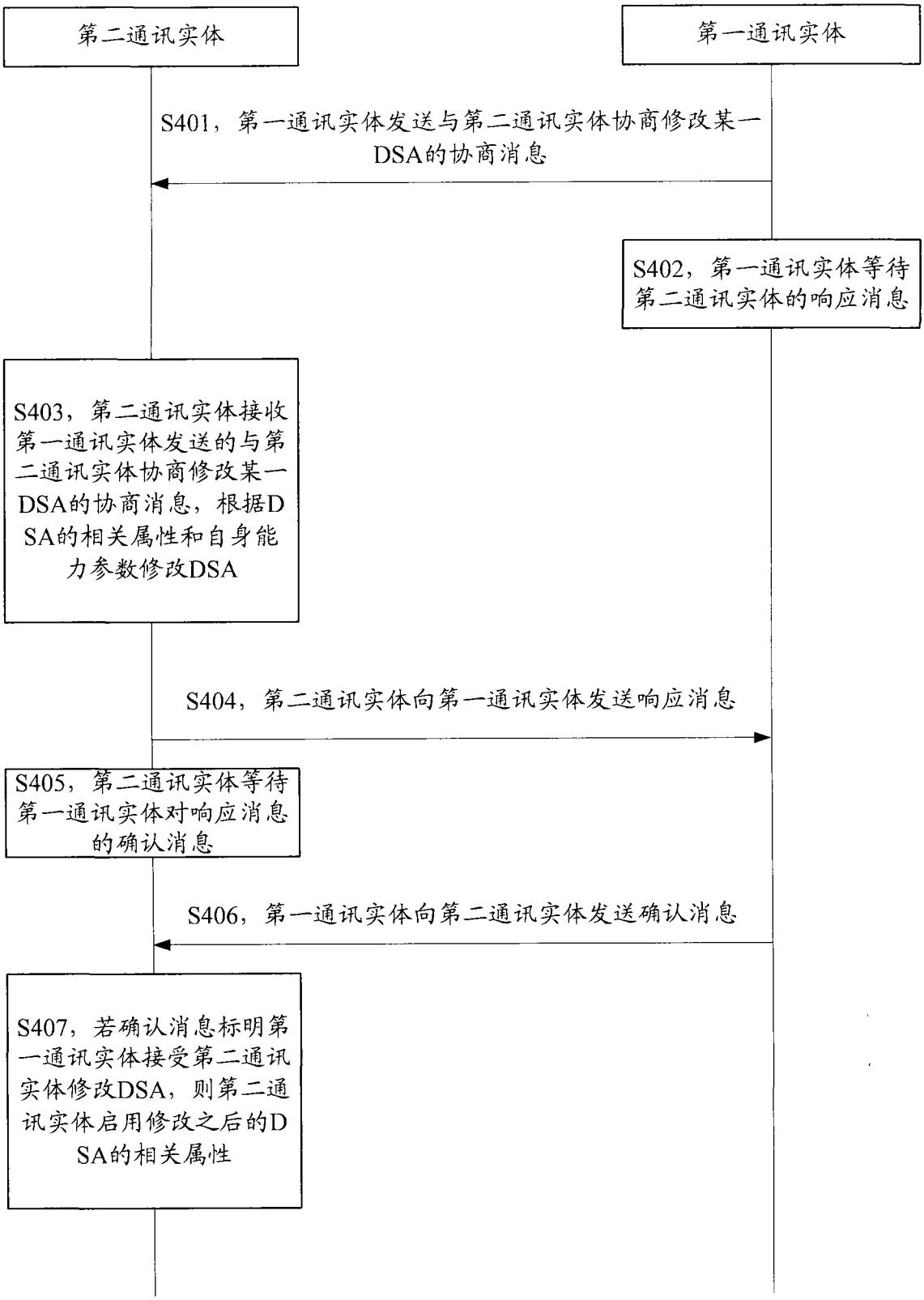

第二通讯实体
第一通讯实体
S401，第一通讯实体发送与第二通讯实体协商修改某一DSA的协商消息
S402，第一通讯实体等待第二通讯实体的响应消息
S403，第二通讯实体接收第一通讯实体发送的与第二通讯实体协商修改某一DSA的协商消息，根据DSA的相关属性和自身能力参数修改DSA
S404，第二通讯实体向第一通讯实体发送响应消息
S405，第二通讯实体等待第一通讯实体对响应消息的确认消息
S406，第一通讯实体向第二通讯实体发送确认消息
S407，若确认消息标明第一通讯实体接受第二通讯实体修改DSA，则第二通讯实体启用修改之后的DSA的相关属性

图 4

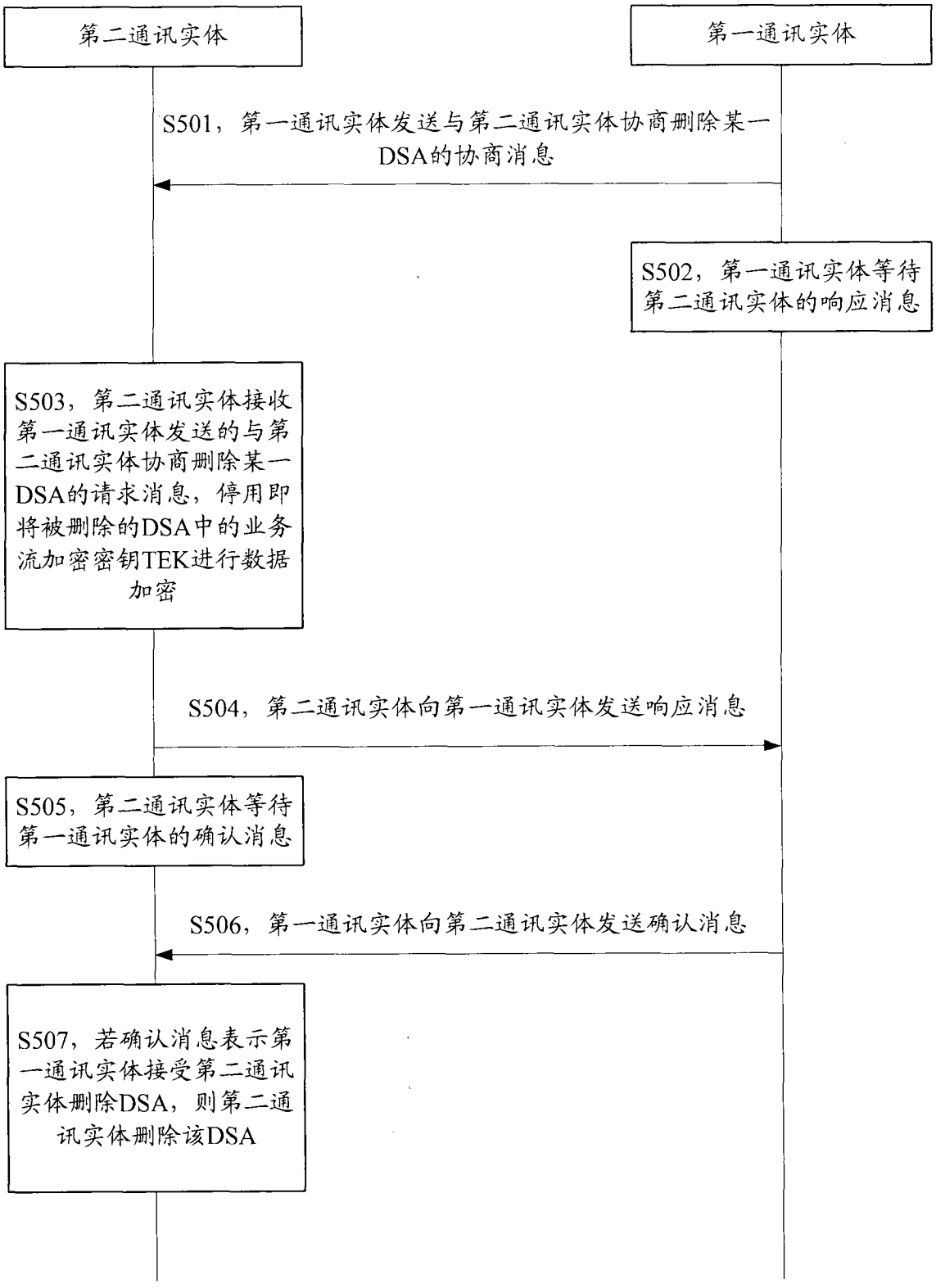

第二通讯实体
第一通讯实体
S501，第一通讯实体发送与第二通讯实体协商删除某一DSA的协商消息
S502，第一通讯实体等待第二通讯实体的响应消息
S503，第二通讯实体接收第一通讯实体发送的与第二通讯实体协商删除某一DSA的请求消息，停用即将被删除的DSA中的业务流加密密钥TEK进行数据加密
S504，第二通讯实体向第一通讯实体发送响应消息
S505，第二通讯实体等待第一通讯实体的确认消息
S506，第一通讯实体向第二通讯实体发送确认消息
S507，若确认消息表示第一通讯实体接受第二通讯实体删除DSA，则第二通讯实体删除该DSA

图 5

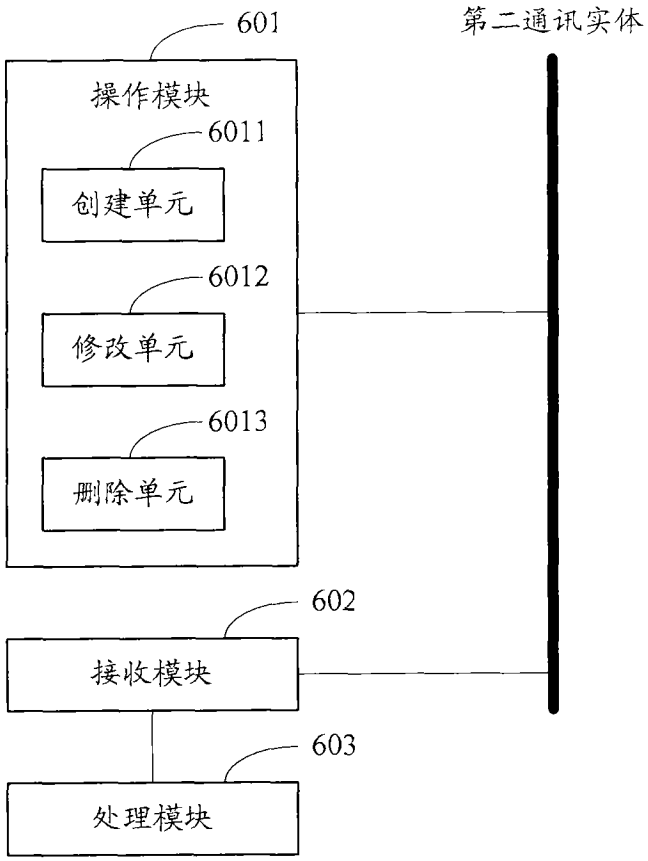

601
第二通讯实体
操作模块
6011
创建单元
6012
修改单元
6013
删除单元
602
接收模块
603
处理模块

图 6

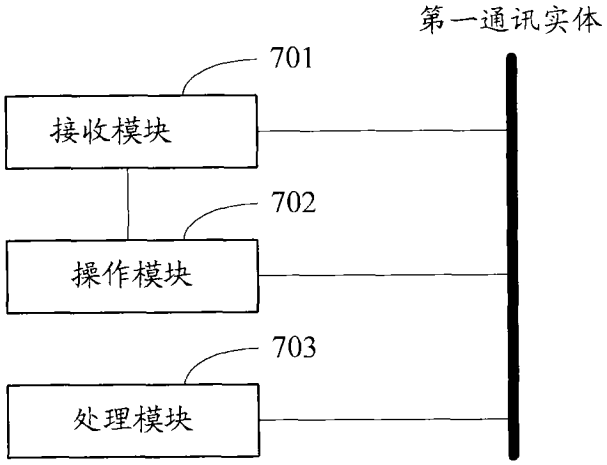

第一通讯实体
701
接收模块
702
操作模块
703
处理模块

图 7