(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 101483588 B
(45)授权公告日 2011.03.09

(21)申请号 200810188993.4

(22)申请日 2002.01.30

(30)优先权数据
01106137.1 2001.03.13 EP

(62)分案原申请数据
02809456.5 2002.01.30

(73)专利权人 西门子公司
地址 德国慕尼黑

(72)发明人 R·赖纳 A·内辰

(74)专利代理机构 中国专利代理(香港)有限公司 72001
代理人 刘春元

(51)Int.Cl.
H04L 12/56(2006.01)
H04L 29/06(2006.01)
H04M 7/00(2006.01)

(56)对比文件
CN 1219055 A,1999.06.09, 全文.
WO 9927686 A1,1999.06.03, 全文.

审查员 常交法

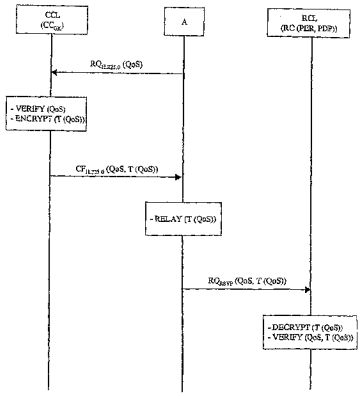
权利要求书 2 页 说明书 14 页 附图 3 页

(54)发明名称

利用已验证的业务质量传输信息的关守和边缘设备

(57)摘要

一种利用已验证的业务质量传输信息的关守和边缘设备，在包括呼叫控制层、资源控制层和至少一个分配给信息传输的端点的通信网中，仅仅在呼叫控制层CCL中费事地验证为了信息传输而求出的QoS要求。随后从中形成加密编码的令牌，并通过该端点传输到资源控制层上。后者仅仅借助已解密译码的令牌来验证从端点输入的QoS要求。在成功的情况下如下来配置通信网，使得用按本发明已验证的QoS来传输信息。本发明实现了在集成的语音和数据网中有效率地、可靠和正确地提供QoS。尤其避免了资源控制层的已有路由器的广泛的修改。此外，在有规则地重复传输令牌时，所提供QoS的一致性的释放以及信息传输的可靠和正确的计费得到支持。



CN 101483588 B

1. 在包括呼叫控制层、资源控制层和至少一个分配给信息传输的端点的通信网中利用已验证的 QoS 传输信息的方法中使用的关守，其中所述的呼叫控制层用于验证是否有权提出 QoS 要求，所述资源控制层在功能上与所述呼叫控制层分开，并用于配置网络使得所述的信息能利用所要求的 QoS 在网络中被传输，所述关守被分配给所述呼叫控制层且具有以下装置：

- 用于验证是否有权为信息传输提出所确定的 QoS 要求的装置；

- 用于在考虑已验证的 QoS 要求的条件下，形成至少一个加密编码的令牌的装置；

- 用于将所述令牌传输到被分配给所述信息传输的端点上的装置，其中由所述的端点将所述已验证的 QoS 要求和加密编码的令牌传输到被分配给所述的资源控制层的边缘设备上，该边缘设备包括：解密译码所述令牌的装置；借助所解密译码的令牌来检验被验证的 QoS 要求的正确性的装置；在考虑所检验的 QoS 要求的条件下配置所述的通信网，使得使用所述已验证的 QoS 来传输所述的信息的装置。

2. 按权利要求 1 的关守，其装置被构造使得由所述的呼叫控制层重复地将令牌传输到所述的端点上，并从那里转送到所述的资源控制层上。

3. 按权利要求 2 的关守，其装置被构造使得由所述的呼叫控制层有规则地以秒的间隔重复地将令牌传输到所述的端点上，并从那里转送到所述的资源控制层上。

4. 按权利要求 1 或 2 的关守，其装置被构造使得将一个其值可变化的信息插入所述加密编码的令牌中。

5. 按权利要求 4 的关守，其装置被构造使得将一个随机数和 / 或一个时标作为所述其值可变化的信息插入所述加密编码的令牌中。

6. 按权利要求 1 或 2 的关守，其装置被构造使得在已有的信令消息中，在所述呼叫控制层与端点之间传输所述加密编码的令牌。

7. 按权利要求 6 的关守，其装置被构造使得在被构造为保持激活消息和 / 或用于刷新所述 QoS 要求的消息的已有的信令消息中传输所述加密编码的令牌。

8. 按权利要求 1 或 2 的关守，其装置被构造使得在成功验证所述的 QoS 要求时由所述的呼叫控制层启动对所述信息传输的计费。

9. 按权利权要求 8 的关守，其装置被构造使得在结束所述信息传输之后由所述的呼叫控制层终止所述的计费，并终止将加密编码的令牌传输到所述的端点上。

10. 按权利要求 1 或 2 的关守，其装置被构造使得借助一个对称的密钥来实现所述的加密编码。

11. 在包括呼叫控制层、资源控制层和至少一个分配给信息传输的端点的通信网中利用已验证的 QoS 传输信息的方法中使用的边缘设备，其中所述的呼叫控制层用于验证是否有权提出 QoS 要求，所述资源控制层在功能上与所述呼叫控制层分开，并用于配置网络使得所述的信息能利用所要求的 QoS 在网络中被传输，所述通信网还包括被分配给所述呼叫控制层且具有以下装置的关守：用于验证是否有权为信息传输提出所确定的 QoS 要求的装置；用于在考虑已验证的 QoS 要求的条件下，形成至少一个加密编码的令牌的装置；用于将所述令牌传输到被分配给所述信息传输的端点上的装置，其中由所述的端点将所述已验证的 QoS 要求和加密编码的令牌传输到被分配给所述的资源控制层的所述边缘设备上，该边缘设备包括：解密译码所述令牌的装置；借助所解密译码的令牌来检验被验证的 QoS 要求

的正确性的装置；在考虑所检验的 QoS 要求的条件下配置所述的通信网，使得使用所述已验证的 QoS 来传输所述的信息的装置。

12. 按权利要求 11 的边缘设备，其装置被构造使得在已有的信令消息中，在所述端点与资源控制层之间传输所述加密编码的令牌。

13. 按权利要求 12 的边缘设备，其装置被构造使得在被构造为保持激活消息和 / 或用于刷新所述 QoS 要求的消息的已有的信令消息中传输所述加密编码的令牌。

14. 按权利要求 11 或 12 的边缘设备，其装置被构造使得借助一个对称的密钥来实现所述的解密译码。

利用已验证的业务质量传输信息的关守和边缘设备

[0001] 本申请是申请日为 2002.1.30、申请号为 02809456.6、发明名称为“在通信网中利用已验证的业务质量传输信息”的发明专利申请的分案申请。

技术领域

[0002] 本发明涉及用于在通信网中利用已验证的 QoS（业务质量）传输信息的方法、计算机程序产品、端点和装置。

背景技术

[0003] 过去已形成了用于传输信息的两种基本的通信网类型：面向分组的数据网和面向线路的语音网。它们还通过它们对 QoS 和安全性的不同要求来互相区分。

[0004] 按前后关系来不同地规定 QoS- 也称为业务质量 -，并随之用各自不同的量度来评价 QoS。用于测量业务质量的量度的公知实例是所传输信息的数量（带宽）、未被传输信息的数量 (Loss Rate 丢失率）、传输时的 - 必要时平均的 - 时间上的延迟 (Delay)、在各两次信息传输之间的通常间隔的 - 必要时平均的 - 偏差（延迟抖动）、或根本不允许用于传输的信息的数量（阻塞率）。

[0005] 安全性譬如包括用户的鉴权和委托、以及所传输信息的完整性和保密性。此时，鉴权是明确识别发送的用户、委托是分配特许、完整性是保证未失真的信息、和保密性是加密编码信息，使得第三方不能理解信息的内容。

[0006] 在加密编码时区分对称的和非对称的加密编码。在编码和译码时的比较中，对称的加密编码方法比非对称加密编码方法是显著地更快的。在对称的加密编码时，发送器和接收器通常分享一个共同的机密 - 也称为‘密钥’或‘Key’-，借助该密钥来编码和译码所加密编码的信息。在非对称的加密编码时，每一方具有一个专用的机密（‘专用密钥’），与该专用的机密匹配地生成一个公知的密钥（‘公用密钥’）。如果由一个发送器用一个接收器的公用密钥来编码信息，则只能由接收器用他的专用密钥来译码该信息。因此保证了所发送信息的保密性，因为只有所述的接收器可以译码该信息。另可选择地，也可以用发送器的专用密钥来编码信息，并由任何接收器用发送器的公用密钥来译码该信息。所述的发送器因此可靠地被鉴权，因为只有当使用仅发送器知道的专用密钥实现所述的信息时，译码才能成功。这种进行方式也称为‘数字签名’或‘签名’。在此，也采用按 ITU 标准 X.509 的所谓的‘证书’。在此分别涉及一个由委托中心或认证当局认证的用户公用密钥。譬如如果通信伙伴还不知道伙伴的证书，或为了加速处理，则有时也在带内传输证书。

[0007] 通过加密编码的保密原理的一个例外是所谓的主权监听 - 也称为合法截取 (Lawfull Interception)-，譬如在侦查犯法行为时可以由国家治理当局和 / 或法院来安排该监听。高质量的安全性方案必须安排一种重新废除已有保密机制的途径，以便实现国家安排的监听。这譬如可以通过公布所采用的密钥来实现。在此，将‘密钥恢复’理解为已丢失密钥的重构，而将譬如由所委托和值得信赖的第三方主管部门使用主权监听用的密钥称为‘Key Escrow（密钥由第三方保存）’。

[0008] 面向线路的语音网是按传输在专业界也称作为‘通话’、‘呼叫’、或‘会话’的连续流动的（语音）信息设计的。在此通常用高的业务质量和安全性来实现信息的传输。譬如没有延迟时间波动（延迟抖动）的一种极小的－譬如 200ms 的－延迟对于语音是重要的，因为语音在接收设备中再现时要求连续的信息流。所以不能通过再次传输未传输的信息来补偿信息损失，并在接收设备中该信息损失通常导至在声音上可以感觉到的劈拍声。语音的传输在专业界泛泛地也称为‘实时（传输）业务’，或也称为‘Realtime-Service’。通过语音网的相应设计和规划来达到所述的业务质量，其中，传输容量本身由于面向线路而原则上不受到波动。譬如通过将语音网对未许可的第三方从空间和组织上进行相应的隔离来实现安全性。因此譬如语音网的主管权过去常常掌握在国家的手中，因而譬如可以在很大程度上排除由第三方进行的窃听。

[0009] 面向分组的数据网是按传输在专业界也称作为‘数据分组流’的分组流来设计的。在此通常不必保证高的业务质量。没有保证的业务质量地进行譬如带有时间上波动的延迟的数据分组流的传输，因为数据分组流的各个数据分组通常以它们的网络接入的顺序被传输，即由一个数据网要传输的分组越多，时间的延迟则越大。所以数据的传输在专业界中也称为无实时条件的传输业务，或也称为‘Non-Realtime-Service（非实时业务）’。安全性起着次要的作用。在譬如象局域网 (LAN) 或公司内部网 (Corporate Network 公司网－也称为虚拟专用网 (VPN)) 的较小的网络中，大多通过网络的空间上的隔离来实现该安全性，因为在这些网络中人们只能找到从一开始就被特许的用户（所谓的‘friendly unsers 友好的用户’）。

[0010] 当今最熟悉的数据网是因特网。因特网是作为开放的（长距通信）数据网来设计的，该数据网具有用于连接不同制造商的（大多为局域和地区的）数据网的开放的接口。所以主要的注意力迄今放在提供与制造商无关的传输平台上。用于保证业务质量和安全性的合适的机制起着次要的作用。所以当今首先用分散的、位于通向因特网接口上的过滤设备－也称为‘防火墙’－来实现提高的安全性。但是还根本不存在网络内部的业务质量机制和安全性机制。尤其是在公知的基于 IP 的语音网和／或数据网中密钥恢复和 Key Escrow 是未公开过的。

[0011] 在面向线路的语音网和面向分组的数据网会聚的过程中，同样在面向分组的数据网中实现语音传输业务，和未来也实现譬如象传输移动图像信息那样的宽带业务，即在会聚的语音数据网中面向分组地，也就是以分组流来实现迄今通常面向线路地所传输的实时业务的传输。这些分组流也称为‘实时分组流’。在此产生以下的问题，需要高的业务质量和安全性来用于面向分组地实现实时业务，以便该传输是可以与面向线路的传输在质量上相比较的，而现代的数据网以及尤其是因特网未安排用于保证高业务质量和安全性的合适的机制（为了规定与业务有关的 QoS 等级也请参阅 ITU 标准 H.323- 附件 N，草案 (02/2000)，″ 在 H.323 系统中端对端的 QoS 控制和信令″，临时文件 126Rev1(TD126rev1.doc)，研究小组 16，日内瓦，2000 年 2 月 7 日 -2 月 18 日，附件 V，章节 10.x.2.4，表 2)。

[0012] 以下集中论述因特网中的语音传输。但是这不是主要的限制，因为业务质量和安全性要求不是专门为因特网构成的，而是一般适用于所有类型的数据网。这些业务质量和安全性要求与数据网的具体方案无关。分组因而可以被构成为因特网分组、X.25 分组或帧中继分组，但是也可以被构成为 ATM 信元。首先当在分组中传输消息时，它们则有时也称为

‘消息’。数据分组流和实时分组流在此是通信网中所传输业务流的实施例。也就是在应用无通信连接的传输技术的面向分组的网络中，业务流也称为‘通信连接’。譬如在 TCP/IP 中借助所谓的流来实现信息传输，尽管 IP 具有无通信连接的特性，但发送器和接收器（譬如网络服务器和浏览器）也在逻辑抽象的层上通过这些流来互相连接，即流也逻辑抽象地表示了通信连接。

[0013] 在国际标准化委员会 IETF(Internet Engineering Task Force) 和 ITU(International Telecommunications Union 国际电信联盟）中，对于语音和图像信息通过面向分组的 IP 网（譬如因特网）- 也称为’VoIP’- 的传输说明了多个体系结构。所有这些的共同之处在于，呼叫控制层和资源控制层在功能上是互相分开的。

[0014] 呼叫控制层包括一个（可选的）呼叫控制器，给该呼叫控制器还分配了以下的功能：

[0015] - 地址转换：将 E.164 电话号码和另外的同义名地址（譬如计算机名）转换成传输地址（譬如因特网地址）。

[0016] - 允许控制（可选的）：原则上的合法性控制，（譬如有 VoIP 能力的）设备是否和在什么范围中允许使用所述的通信网。

[0017] - 带宽控制（可选的）：传输容量的管理。

[0018] - 区域管理：注册（譬如有 VoIP 能力的）设备，并提供所有在呼叫控制器中注册的设备用的上述功能。

[0019] 可选的还可以按情况给呼叫控制器分配以下的功能：

[0020] - 呼叫控制信令：由至少一个呼叫控制器交换所有的信令消息，即所有的设备仅通过所述的呼叫控制器发送和获得信令消息。禁止在设备之间直接交换信令消息。

[0021] - 呼叫认可：进出呼叫的合法性控制。

[0022] - 带宽管理：控制可以同时使用通信网的设备的允许数量。

[0023] - 呼叫管理：已有通话清单的管理，以便譬如当不能由设备本身生成占用信号时可以生成该占用信号。

[0024] - 同义名地址修改：譬如用 H.225.0 消息 ACF 返回已修改的同义名地址（地址证实）。在通信连接建立时的端点必须使用该地址。

[0025] - 拨号数字转换 (Dialed Digit Translation)：将所选的数字翻译成 E.164 电话号码，或翻译成来自专用编号表中的号。

[0026] 当今，本身不能执行这种功能的设备的、由呼叫控制器引起的带宽预留问题是被搁置的，并且" 有待进一步研究" （请参阅 H.323 草案 v4(07/2000)，章节 6.4)。

[0027] 呼叫控制器的实例是由 H.323 标准族中的 ITU 所建议的‘关守’，或由 IETF 所建议的‘SIP-Proxy(SIP 代理)’。如果一个较大的通信网被划分成多个域 - 也称为区域 -，则可以在每一个域中安排一个独立的呼叫控制器。没有呼叫控制器也可以运行域。如果在一个域中安排了多个呼叫控制器，则只应激活这些呼叫控制器中的唯一一个。呼叫控制器从逻辑的角度可以被看作为与设备分开的。但是物理上它不必被实现在独立的呼叫控制器设备中，而是也可以被安排在通信连接的每一个端点中（譬如被构成为 H.323 端点：终端设备、网关、多点控制单元等等），或也可以被安排在原先为了程控的数据处理而构成的设备（譬如：计算机、个人计算机等等）中。物理上分布式的实现也是可能的。

[0028] 资源控制层包括一个资源控制器作为中央元件，给该资源控制器还分配了以下的功能：

[0029] - 容量控制：譬如通过控制各个分组流的传输容量来控制通过分组流输送给通信网的业务量。

[0030] - 策略激活（可选的）：必要时在通信网中对于一个优先的分组流预留资源，用于它的传输。

[0031] - 优先等级管理（可选的）：如果已经用优先等级标记了分组，则在所述的分组中按它们的分组流的优先等级设置、控制和必要时纠正优先等级标识。

[0032] 资源控制器也称为‘策略判定点 (PDP)’。它通常实现在所谓的‘边缘路由器’之内 - 也称为‘边缘设备’、‘接入节点’、或在向因特网业务供应商分配时也称为‘供应商边缘路由器 (PER)’。另可选择地，PER 也可以只作为代理起作用，并将与资源控制器有关的信息转送到资源控制器被实现在其上的独立的服务器上。

[0033] 现以在两个构成为用户终端设备的 VoIP 设备之间的呼叫建立为例，阐述呼叫控制器和资源控制器按 IETF 和 ITU 协议的原则性协作（请参阅 H.323 草案 v4(07/2000)，附件 II）。

[0034] 在本来的呼叫建立之内或部分地甚至时间上在此之前，在（譬如通过因特网业务供应商）将终端设备拨入 IP 网时执行以下的步骤：鉴权、委托和（开始）计费。

[0035] 通常通过访问存储有所有具有其标记、通行字、权利等等的使用者的用户数据库来实现该所谓的’AAA’功能性。该访问是缓慢而比较复杂的。在当今的″ Best Effort″ IP 网中，在使用者的拨入期间该 AAA 过程通常只进行一次。在采用呼叫控制器时，如果终端设备在因特网业务供应商的呼叫控制器（譬如 SIP 代理或 H.323 关守）处注册，则进行另一种鉴权。按照 H.323 草案 v4(07/2000)，在所分配的关守处按照 RAS（注册、准许、状态）协议实施终端设备的这种鉴权或注册。在 ITU 标准 H.225.0 中说明了所述的 RAS 协议。在这当中也安排了一个机制，其中，在某个时间之后取消一次性进行的注册，并只有当它及时重新被刷新时，该注册才继续存在（请譬如参阅 H.225.0(02/98) 章节 7.9.1 和 7.9.2，在用于设置注册寿命的消息 RegistrationConfirm RCF（证实注册）中的参数 timetolive（寿命），和在用于刷新、即延长已有注册的寿命的消息 Registration Request RRQ（注册请求）中的参数 keepAlive（保持激活））。

[0036] 在第一步骤中用户的终端设备交换它们的能力（譬如所支持编解码器的清单），以便确定所需要的资源（譬如带宽）和所要求的 QoS（譬如延迟、抖动），通常以此来开始本身的呼叫建立。在语音电话情况下终端设备譬如被构成为 IP 电话，处于在线视频情况下，终端设备中的一个譬如可能是因特网业务供应商网络中的内容服务器或应用服务器。

[0037] 要么直接在终端设备之间，要么在呼叫控制器的交换情况下来实现信令消息的交换。此时，在每次呼叫时对于每个终端设备和对于每个传输方向而专门地确定采用哪个变型方案。譬如在 H.323 草案 v4(07/2000) 中第一变型方案被称为‘直接端点呼叫信令’，而第二变型方案被称为‘关守路由呼叫信令’。在直接端点呼叫信令中必要时将所选出信令消息的备份传输到呼叫控制器上。呼叫控制器因此常常知晓在终端设备之间商定的资源要求和 QoS 要求。但是该呼叫控制器自己不主动地影响或验证这些要求。

[0038] 在可选的第二步骤中，可以将如此商定的资源要求和 QoS 要求直接从用户的终端

设备传输到它们所分配的资源控制器上。在控制资源要求和 QoS 要求之后由资源控制器将确认（或拒绝）回送到终端设备上。

[0039] 在同样为可选的第三步骤中，在网络中的边缘路由器中，和必要时在其它的路由器中激活一种‘策略’，这些路由器使用该策略来控制和确保，由所述终端设备所促成的业务位于所述要求已规定的界限之内。这种预留机制的实例是 RSVP（资源预留协议）。

[0040] 发送多个消息用于实施所述的三个步骤，这些消息仅仅用于相互协调所参与的部件，但是不用于在终端设备之间传输″本来的信息″。这些用所述消息传输的信息通常称为″信令信息″、″信令数据″、或简单地称为″信令″。此时应广泛地理解所述的概念。因此譬如除了信令消息之外也包括了按 RAS 协议的消息、按 ITU 标准 H.245 的用于控制已有通话的有用信道的消息、以及所有其它相似构成的消息。譬如在标准 H.225.0″在 LAN 的不保证 QoS 基础上的媒体流的分组和同步″，2000 中说明了按 ITU 的通信连接建立（呼叫建立）和通信连接断开（呼叫断开）用的信令协议，该信令协议遵照 RFC2453bis 中的 IETF，″ SIP：会话初始化协议″，draft-ietf-sip-rfc2453bis-02.txt，09/2000。为了区别于信令，所述的″本来信息″也称为‘有用信息’、‘媒体信息’、‘媒体数据’、或简单地称为‘媒体’。

[0041] 在此，将‘带外 (out-of-band)’理解为在另外路径 / 媒体上传输信息（譬如密钥），该路径 / 媒体不同于通信网中为了传输信令信息和有用信息而安排的路径。尤其这其中包括了设备在现场的一种本地配置，譬如使用本地的控制装置进行该配置。与此相反地，在‘带内 (in-band)’情况下，在相同的路径 / 媒体上、必要时逻辑上与所观察的信令信息和有用信息分开地传输信息。

[0042] 因此在这里概括地将（传输）连接的建立，呼叫信令（有时具有保密性）的和其它信号交换的建立、以及（语音）数据传输的开始理解为呼叫建立。在 ITU 标准 H.323 中，将具有微小延迟时间和短往返时间的、快速有效的通信连接建立也称为‘快速连接’，该通信连接建立具有尽可能少的附加信息流或信号交换。

[0043] 基于迄今所述的可以了解到，只有在下列前提下才认可 VoIP 的实现：

[0044] - 对于用户主要的是，像在语音网中那样，在集成的语音数据网中以相同的业务质量 (QoS) 来传输所属的信令数据以及构成为语音的媒体数据。

[0045] - 对于网络经营者重要的是，象在语音网中那样，以相同的安全性和质量来对所传输的通话计费。

[0046] 本身不能实施该功能的设备的、由呼叫控制器所引起的带宽预留问题目前是搁置的，并且″有待进一步研究″（请参阅 H.323 草案 v4(07/2000)，章节 6.4）；可靠计费的特征完全未被谈及。在用于 QoS 的研究工作范围内，在 ITU 标准 H.323- 附件 N，草案 (02/2000)，″ H.323 系统中的点对点 QoS 控制和信令″，临时文件 126Rev1(TD126rev1.doc)，研究组 16，问题 13/16 和 14/16，日内瓦，2000 年 2 月 7 日 -2 月 18 日，中公布了一种具有以下特征的用于 QoS 控制的机制：

[0047] - 端点有能力既对于离开的，也对于到达的媒体流指明 QoS 要求（附件 N 草案 (02/2000)，章节 3.2，款 1）。

[0048] - 要么在每次呼叫时端点指明 QoS 要求，要么在业务供应商处预先设置了所述的 QoS 要求，并可以选择地在每次呼叫时用一个专门的 QoS 要求来改写所述的 QoS 要求（附件

N 草案 (02/2000)，章节 3.2，款 2)。

[0049] - 在关守中应可以注册所谓的用户专门的 QoS 简要表。这些 QoS 简要表用于委托一种 QoS 要求，其方式是由它们确定 QoS 水平，某个用户譬如根据其与某个业务供应商签署的合同而允许要求这些 QoS 水平（附件 N 草案 (02/2000)，章节 3.3，款 1)。

[0050] - 关守应该可以确定，是否可以满足端点的 QoS 要求（附件 N 草案 (02/2000)，章节 3.3，款 3)。

[0051] - 关守应该能够通过与传输网（即资源控制层）的 QoS 机制的（直接）通信，来激活所述传输网的能力、支持 QoS 要求、命令传输网、按预先规定的 QoS 要求建立专门的通信连接、提供合适的委托。此时，在编辑程序 (Editor) 的脚注中阐明了，由关守通过端点的间接控制可能是一个值得考虑的替代措施。但是未进一步阐明以此指的是何种控制，还未给出提示，可以如何构成该间接的控制（附件 N 草案 (02/2000)，章节 3.3，款 6)。

[0052] - 在此，关守应该确定，端点的 QoS 要求是否位于它的 QoS 简要表的界限之内，并是否依赖于此来授予或拒绝用于建立通信连接的委托（附件 N 草案 (02/2000)，章节 3.3，款 7)。

[0053] - 用于 QoS 控制的 H.323 机制含有以下的功能单元：用于要求所希望 QoS 水平的端点 QoS 实体 (EPQoSSE)；用于管理策略和用于委托 QoS 水平的 QoS 策略实体；用于按由 QoSPE 所规定的策略来交换 QoS 要求的 QoS 业务管理器 (QoSM)；用于将一个数量的策略和过程应用到一个数量的传输资源上的资源管理器 (RM)，该应用的目的在于，由此所分配的资源足够用于在处于 RM 控制之下的域之内保证所要求的 QoS（附件 N 草案 (02/2000)，章节 4.3)。

[0054] - 在端点之内布置了 EPQoSE、在 H.323 域之内布置了 QoSM 和 QoSPE、和在传输域之内布置了 RM。EPQoSE、QoSM 和 QoSPE 被分配给呼叫控制层，而 RM 被分配给资源控制层。这些功能单元之间的关系网安排了一个中央 QoSM，EPQoSE、QoSPE 和 RM 各自与该中央 QoSM 存在双向关系。但是在 EPQoSE、QoSPE 和 RM 之间未安排直接的关系（附件 N 草案 (02/2000)，章节 4.3，附图 3)。

[0055] 但是在譬如象因特网那样的集成的语音数据网中的技术实现时出现了以下的问题，迄今无论在 IETF 和 / 或 ITU 的标准和草案中，还是在已公开的实施中没有或仅不充分地解决了这些问题：

[0056] P1. 尽管动态地对每个呼叫和使用者实行所述的要求，所述的 PER(RC，PDP) 如何能够有效地实施资源要求和 QoS 要求的鉴权和委托？外加于此的困难在于，在 PER 和其它路由器中的预留通常是" 软的"，也就是必须以有规则的时间间隔（数量级：秒）来刷新预留，譬如其方式是重新将要求发送到资源控制层上。非常专门地为一种用途或一个使用者制定的、或在 PER(RC、PDP 等等）中需要很多计算时间的鉴权和委托机制从一开始就被排除在外（标定问题、实时问题）。PER 和 ISP 的其它路由器今天不具有与使用者有关的信息，并在未来也不具有这些信息，因为分配给它们的任务主要在于，给 IP 分组选择路由，并按策略来决定优先等级。

[0057] P2. 如何能够可靠地实施鉴权和委托，使得人们可以据此计费（在语音网中计费模型完全或部分地根据所预留的资源，而与它们的实际使用无关）？如果应该仅仅检验整个的资源预留，以便防止网络中的过载，则显著地出现较小的安全性要求。安全性也是必要

的，因为参与呼叫的两个使用者发送出资源要求和 QoS 要求，但是必要时只应给两个使用者之一计费。

[0058] P3. 在采用呼叫控制器时如何能够确保，使用者的终端设备将准确的、即由呼叫控制器确认的资源要求和 QoS 要求发送到资源控制层上？由于滥用或技术缺陷，参与通信连接的终端设备可能各自发送任意的要求！

[0059] P4. 尽管两个终端设备通常询问完全不同的 PER，如何确保两个终端设备的资源要求和 QoS 要求的一致的释放？因此譬如尽管主叫的和支付通话费用的用户已经终止通话，被叫的用户在他这方面可能直至他的网关仍继续保持所述的预留，并通过给出另外的 IP 地址还从服务器下载数据。如果计费譬如建立在所传输数据的数量的基础上，所述的网关则可能还将这些数据算入到上一次通话中，即必要时也算入该计费中。这对于一个 ISP 的两个 PER 已是一个问题，在具有不同 ISP 的 PER 的域间情况下这变得更为困难。

[0060] 显然，这些问题的解决办法对于由 IETF 和 ITU 所建议方案的实际可使用性是必不可少的，并因而主要地决定了网络体系结构。

[0061] 迄今未适当地（即用完全象所述体系结构方案本身那样的一般性的措施）解决上述问题。要么采用不可一般化的专门解决办法，因为它们譬如以某个制造商的网元为前提，要么通过在灵活性、动态性或资源预留和 QoS 保证的效率上的限制来回避所述的问题 P1-P4。在某些条件下，譬如在较小的公司网中也根本不出现上述问题，在这些公司网中人们可以从使用者（″友好的用户″）出发，这些使用者从一开始（即没有鉴权和委托）就有权将 IP 网仅用于为此所安排的目的（即没有监控），并对于这些使用者譬如由于网络费用的内部结算而不产生计费（即没有计费计费）。

[0062] 譬如在欧盟的天鹰座 (Aquila) 项目中奉行一种专用的措施：使用者在他的终端设备（譬如 PC) 上具有用其可以报告资源需求的应用程序。由网络中的专门的 RC 服务器来处理该资源要求，该 RC 服务器借助数据库查询来确定使用者的特许（鉴权和委托）。这里的缺点是专用的应用程序、以及通常很缓慢和动态费事的附加的数据库查询，以及要么（除了在使用者拨入时的访问之外）要求进一步访问 ISP 的 AAA 数据库（如果 ISP 和呼叫控制器的经营者不是同一个，那么这将表现为不受欢迎的安全性风险），要么以一个与 AAA 数据库必须一致的第二数据库为前提。此外，不利之处还在于，在后处理中为了计费必须进行呼叫控制器的数据与来自 RC 服务器的数据的相关。因此排除了‘热记帐’（即呼叫期间的计费信息）。在第一次预留期间也仅一次性进行使用者的可靠的鉴权，因为随后使用 PER 中的静态策略进行工作。人们因此回避了路由器中软预留的原则，该原则已由 IETF 用协议 RSVP 建议过。因此在该措施中问题 P1、P3 和 P4 仍未被解决。

[0063] 业务质量网络公司，都柏林，爱尔兰，现在实现着一种有 QoS 能力的 IP 网。在此，由 ISP 静态地进行策略调节（即没有动态的资源预留）。这是一个对于公司客户可接受的建议，因为在公司之内可以查清资源需求，基于整个公司业务的聚集性，要求简要表在时间上大致是恒定的，以及由于只有公司雇员具有通向网络的通道，因此可以取消使用者的委托。但是这对于想给私人客户或 SOHO(Single OfficeHome Office（单个办公室家庭办事处）) 客户提供具有 QoS 能力的 IP 网的 IPS 来说，还不是解决办法。问题 P1 至 P4 仍未解决，因为在该专门的业务模型中相应的限制不是特别不利的，或未提供技术的解决办法。

发明内容

[0064] 本发明的任务在于找到一个至少问题 P1 至 P4 之一用的合适的解决办法。通过以下方案来解决该任务。

[0065] 根据本发明的在包括呼叫控制层、资源控制层和至少一个分配给信息传输的端点的通信网中利用已验证的 QoS 传输信息的方法中使用的关守，其中所述的呼叫控制层用于验证是否有权提出 QoS 要求，所述资源控制层在功能上与所述呼叫控制层分开，并用于配置网络使得所述的信息能利用所要求的 QoS 在网络中被传输，所述关守被分配给所述呼叫控制层且具有以下装置：

[0066] - 用于验证是否有权为信息传输提出所确定的 QoS 要求的装置；

[0067] - 用于在考虑已验证的 QoS 要求的条件下，形成至少一个加密编码的令牌的装置；

[0068] - 用于将所述令牌传输到被分配给所述信息传输的端点上的装置，其中由所述的端点将所述已验证的 QoS 要求和加密编码的令牌传输到被分配给所述的资源控制层的边缘设备上，该边缘设备包括：解密译码所述令牌的装置；借助所解密译码的令牌来检验被验证的 QoS 要求的正确性的装置；在考虑已验证的 QoS 要求的条件下配置所述的通信网，使得使用所述已验证的 QoS 来传输所述的信息的装置。

[0069] 根据本发明的在包括呼叫控制层、资源控制层和至少一个分配给信息传输的端点的通信网中利用已验证的 QoS 传输信息的方法中使用的边缘设备，其中所述的呼叫控制层用于验证是否有权提出 QoS 要求，所述资源控制层在功能上与所述呼叫控制层分开，并用于配置网络使得所述的信息能利用所要求的 QoS 在网络中被传输，所述通信网还包括被分配给所述呼叫控制层且具有以下装置的关守：用于验证是否有权为信息传输提出所确定的 QoS 要求的装置；用于在考虑已验证的 QoS 要求的条件下，形成至少一个加密编码的令牌的装置；用于将所述令牌传输到被分配给所述信息传输的端点上的装置，其中由所述的端点将所述已验证的 QoS 要求和加密编码的令牌传输到被分配给所述的资源控制层的所述边缘设备上，该边缘设备包括：解密译码所述令牌的装置；借助所解密译码的令牌来检验被验证的 QoS 要求的正确性的装置；在考虑已验证的 QoS 要求的条件下配置所述的通信网，使得使用所述已验证的 QoS 来传输所述的信息的装置。

[0070] 许多优点是与该解决办法相联系的：

[0071] - 在资源控制层中可以取消 QoS 要求的重新的、复杂而动态上要求苛刻的鉴权和委托，因为按本发明借助解密译码的令牌来实现该鉴权和委托。使用者数据库不必被复制，或不必按照附加的周期性进行的查询的处理来设计。呼叫控制层和资源控制层中的机密的共同的占有实现了对称加密编码方法的采用。这些方法在动态上是比非对称方法显著地更快的。总之可以确定，本发明本身已经是很有效的。所述的机密与专门的使用者、专门的呼叫、QoS 要求或稍后的周期性刷新要求无关。管理机密的管理花费因而是极小的，并且不随 ISP 使用者的数量而增长。将统一工作的加密编码方法纳入到呼叫控制层（譬如关守）和资源控制层（譬如 PER）中在技术上是简单的。本发明设备（呼叫控制器，资源控制器）和装置的管理和实现因而也是有效率的 - 问题 P1。

[0072] - 用于令牌的加密编码和解密译码的加密编码方法的采用不仅在技术上，而且也在法律上是安全的。在足够良好地加密编码的要求情况下，因此甚至于可以进行计费 - 问题 P2。

[0073] - 在相应考虑的情况下（譬如纳入所验证的QoS要求，或至少纳入所验证QoS要求的主要部分），可以无真正更多花费地（即有效率地）来有利地排除在终端设备之间所交换的要求和实际由终端设备所发送的要求之间的失真，其方式是，在形成加密编码的令牌时考虑在呼叫控制层中验证的QoS要求，并因此在令牌的解密译码之后所验证的QoS要求对于资源控制层是已知的。所述的QoS要求因而也是准确的 - 问题P3。

[0074] - 所述的解决办法是完全符合标准的，它不需要任何附加的专用协议或消息。本发明是普遍和方案性地可互操作的，因为它与具体的解决办法无关。它既可以应用于H.323网，也可以应用于SIP网。这使得本发明既在H.323中，也在SIP中都成为一种全面的解决办法。这是重要的和因此是特别有利的，因为象过去已指明的那样，市场较少地接受制造商专门的解决办法。

[0075] - 只须对呼叫控制层和资源控制层统一选择加密编码方法。端点不受此影响。所述的解决办法所以允许与使用者终端设备上的不同应用程序的互操作性。

[0076] - 可以改善加密编码方法（新的方法、较长的密钥、更严厉的法律要求等等），其方式是ISP仅仅在它的PER(RC、PDP等等）和呼叫控制器（有时也在另一个公司的占有之下）上进行刷新。端点或在其上所执行的应用程序又有利地保持不受影响。

[0077] 按本发明的一个扩展方案，由所述的呼叫控制层重复地，尤其有规则地以秒的间隔重复地将令牌传输到所述的端点上，并从那里转送到所述的资源控制层上。尤其将一个其值可变化的信息、尤其是一个随机数和/或一个时标插入所述加密编码的令牌中。如果将呼叫控制层中的QoS要求扩充了一个动态确定的随机数，则也可以有利地用同一个密钥加密编码或解密译码任何刷新消息。如果将时标插入加密编码的QoS要求中，则有利地确保了端点可以不延迟或存储该已验证的要求，以便在稍后的时刻转送该要求（欺骗特征：在夜间适用较低的费率时收集、而在白天高费率时采用加密编码的要求）。尤其有利的是，如果另一个端点已终止了信息传输，则通过端点中的一个排除了（软）预留的进一步维持。在该情况下由呼叫控制层不发送其它的令牌。ISP的PER和网络中的其它路由器废除（释放）对于具有保证的QoS的信息传输所必要的资源预留。此时，特别良好的优点在于，资源控制层对于该一致的释放不必具有应用程序的任何知识，这些应用程序促成来自或通向端点的IP业务（实例：使用者在因特网中冲浪期间实施IP电话通话。路由器预先不知道，何时必须为实时语音业务预留专门的资源和何时Best-Effort满足所述的使用者）- 问题4。

[0078] 良好的优点是也与以下的内容相联系的，即在已有的信令消息中、尤其在保持激活(KeepAlive)消息和用于刷新所述QoS要求的消息中，在所述端点与呼叫控制层之间，和/或在所述端点与资源控制层之间传输所述加密编码的令牌。如果使用已有的（信令/预留）信号，则在网络中不出现新的消息。此外，附加插入的加密编码的要求对于未参与该技术的网元没有影响（透明）：这些网元象迄今那样只对信号的原来的部分作出反应（与老网元的互操作性）。

[0079] 如果在成功验证所述的QoS要求时由所述的呼叫控制层启动对所述信息传输的计费，则产生特别良好的优点，和必要时在结束所述信息传输之后终止所述的计费，并终止将加密编码的令牌传输到所述的端点上。由于呼叫控制层控制着呼叫的开始和甚至结束（通过端点的动作，譬如挂上电话话筒来触发），因此不仅可以可靠地，而且也可以在时间上精确地进行计费 - 请参阅问题2。

[0080] 如果借助对称的机密，尤其借助对称的密钥来实现所述的加密编码和解密译码，本发明的特点则在于有特别的效率。

附图说明

[0081] 以下借助附图中示出的实施例详述本发明。

[0082] 图 1 展示了用于实施本发明方法的、具有呼叫控制层、资源控制层以及信息传输的两个端点的装置。

[0083] 图 2 展示了附图 1 装置的示范性详述的扩展方案，该装置具有实施本发明方法的程序。

[0084] 图 3 展示了流程图，其中示范性地指明了本发明方法的一个实施方案。

具体实施方式

[0085] 附图 1 中示出了一个用于实施本发明方法的示范性的装置，该装置被实施为具有呼叫控制层 CCL、资源控制层 RCL 以及信息传输的两个端点 A，B 的通信网。构成为对称机密 K_A，K_B 的机密在两个层 CCL，RCL 中得到应用。还示出了两个令牌 T_A，T_B。在此，令牌 T_A（或 T_B）是安排用于用机密 K_A（或 K_B）加密编码地从层 CCL 经过端点 A（或 B）到层 RCL 上的传输。

[0086] 附图 2 中示出了一个附图 1 装置的详细的扩展方案。要强调的是，在这里所表明的实施方案此时尽管它们是部分忠实细节的描述，仍应仅仅被理解为具有示范性的特性和不受限制的。在该扩展方案中层 CCL 包括两个呼叫控制器 CC，其中，分配给端点 A 的呼叫控制器 CC 被构成为关守 CC_{GK}，而分配给端点 B 的呼叫控制器 CC 被构成为 SIP 代理 CC_{SIP}。给所述的关守 CC_{GK} 分配了使用者数据库 DB_A，而给 SIP 代理 CC_{SIP} 分配了用于验证使用者及其权利的使用者数据库 DB_B，譬如使用协议 LDAP（轻型词库访问协议）访问这些使用者数据库。在关守 CC_{GK} 中安排了机密 K_A，在 SIP 代理 CC_{SIP} 中安排了机密 K_B。在两个呼叫控制器 CC 之间必要时交换信令消息。层 RCL 包括一个中央资源控制器 RC。给该中央资源控制器 RC 分配了两个用于在通信网中传输信息的边缘路由器 PER_A，PER_B。在边缘路由器 PER_A 中安排了机密 K_A，在边缘路由器 PER_B 中安排了机密 K_B。在资源控制器 RC 和边缘路由器 PER 之间执行协议 COPS（公用开放策略服务器）。此外，在端点 A 和关守 CC_{GK} 之间应用协议 H.225.0，在端点 A 和边缘装置 PER_A 之间以及在端点 B 和边缘装置 PER_B 之间应用协议 RSVP（资源预留协议），而在端点 B 和 SIP 代理 CC_{SIP} 之间应用协议 SIP（会话初始化协议）。在协议 H.225.0、SIP、RSVP 的标准化消息中各自传输令牌 T_A，T_B。在边缘装置 PER_A 和 PER_B 之间至少采用协议 RSVP、DiffServ 或 MPLS 中的一个。在端点 A 和 B 之间指明了通话 CALL，对于该通话的定性优质的实施需要具有保证的 QoS 的信息传输。在通信网中通过协议 RTP（实时协议）来传输信息。通信网譬如是构成为 IP 网的。对于有关的专业人员来说显然的是，本发明当然可以在譬如象因特网、局内网 (Intranet)、局外网 (Extranet) 那样的其它网络类型中，在局域网 (LAN) 中、或在譬如构成为虚拟专用网 (VPN) 的公司内部网（企业网）中得到应用。在终端设备 A 和 B、呼叫控制器 CC 和边缘装置 PER 中安排了本发明的计算机程序产品 P，这些计算机程序产品各自包括用于由处理机辅助实施本发明方法的软件代码段。此时，也可以可选地在专门的硬件（譬如密码处理机）上执行所述计算机程序产品 P 的部分。

[0087] 附图 3 中，以遵照 ITU 的 H.323 标准族的呼叫 CALL 的、未完全示出的构造（呼叫建立）为例，借助流程图示出了一个本发明方法的实施方案。在图表中指明了用于在端点 A 和层 CCL 之间交换信令数据的标准化的（信令）消息 $RQ_{H.225.0}$，$CF_{H.225.0}$，以及用于向层 RCL 请求 QoS 的（信令）消息 RQ_{RSVP}，这些（信令）消息部分地是如下被修改的，使得本发明方法得到实施。消息 RQ_{RSVP} 取自标准化的协议 RSVP，在 IETF 中已开发了该协议，用于在终端设备 A，B 之间，或从终端设备 A，B 向 IP 网中传输资源要求和 QoS 要求 RQ。

[0088] 以下将关守 CC_{GK}、端点 A 和边缘装置 PER_A 的本发明特性和共同作用作为实例来阐述。在协议 H.225.0 和 RSVP 的相应修改的（信令）消息中传输与本发明有关的信息。在此对于专业人员清楚的是，呼叫控制器 CC 是可以任意构成的，尤其是也可以构成为 SIP 代理 CC_{SIP} 的。附图 2 中对于端点 B 表示了该实施方案。

[0089] 终端设备 A 首先被注册在关守 CC_{GK} 中。由终端设备 A 通过 H.225.0 注册请求 RRG 来申请注册，并由关守 CC_{GK} 用 H.225.0 注册确认 RCF、或用 H.225.0 注册拒收 RRJ 来应答所述的申请。在消息 RRQ 中可能已经含有了一般的 QoS 要求 RQ，该 QoS 要求应对于所有随后的通话 CALL 具有一般的适用性。于是由关守 CC_{GK} 验证（即鉴权，委托等等 ...）端点 A 和必要时的 QoS 要求 RQ。为此借助协议 LDAP 或另外的 DB 查询协议来访问譬如存放在数据库 DB_A 中的使用者专门数据。这些数据也可以包括最高允许的 QoS 要求 RQ，譬如可以按使用者与其 ISP 的合约确定该 QoS 要求 RQ。必要时现在已经求出了允许的当前 QoS 要求 RQ。于是已经可以在消息 RCF 中将该 QoS 要求 RQ 传输到端点 A 上。

[0090] 此外也由关守 CC_{GK} 确定，是否应由它自己来交换呼叫信令（关守路由呼叫信令），或直接在端点 A，B 之间交换呼叫信令（直接端点呼叫信令），必要时使用要关守 CC_{GK} 作出主要改变的通知。虽然端点 A，B 应坚持这些确定；但是如果想防护通信网免受端点 A，B 的错误特性的影响，则必须安排附加的安全机制。

[0091] 在两个端点 A，B 注册之后，在两个终端设备 A，B 之间的呼叫信令，尤其是呼叫建立基本上是可能的。譬如由端点 A 初始化该注册，其方式是用 H.225.0 准许请求 ARQ 来在关守 CC_{GK} 中申请建立通向端点 B 的通话 CALL。该 ARQ 又可以含有一个 QoS 要求 RQ。随即由关守 CC_{GK} 实施有关所述通话 CALL 的鉴权和委托。该鉴权和委托也包括 QoS 要求 RQ 的求取。譬如也可以通过借助其它的 H.225.0 消息所实现的两个端点 A，B 之间的能力商议来求出该鉴权和委托。于是在关守路由呼叫信令的情况下，该鉴权和委托对于关守 CC_{GK} 是直接已知的。在直接端点呼叫信令情况下，可将该鉴权和委托通知给关守 CC_{GK}。由关守 CC_{GK} 验证所求出的 QoS 要求 RQ。

[0092] 现在通过考虑所验证的 QoS 要求 RQ，由关守形成至少一个借助机密 K_A 加密编码的令牌 T。譬如与使用者有关的数据（譬如 IP 地址、端口号等等）、以及所有的资源要求数据和 QoS 要求数据或其主要部分流入该令牌 T 中。按本发明的一种变型方案，在形成令牌 T 时也考虑其值可变化的信息，譬如随机数或时标。可选地，开始通话 CALL 的计费。譬如在 H.225.0 消息 ACF（准许确认）中将加密编码的令牌 T 传输到端点 A 上。在端点 A 中从消息 ACF 中获取和暂存如此传输的令牌 T。由终端设备 B 用消息 CONNECT（连接）给关守 CC_{GK} 指明接受通话 CALL。可以由关守 CC_{GK} 将令牌 T 插入消息 CONNECT 中，该消息 CONNECT 由关守 CC_{GK} 传输到终端设备 A 上用于显示成功的呼叫建立。

[0093] 随后由端点 A 将加密编码的令牌 T 插入否则未改变的标准化 RSVPQoS 要求 RQ 中，

并传输到边缘装置 PER_A 上。由所述的边缘装置 PER_A 借助机密 K_A 将所加密编码的令牌 T 解密译码，并然后用于验证 QoS 要求 RQ 的准确性。只要已经事先在关守 CC_{GK} 和资源控制器 RC 之间未曾进行协调，现在则由边缘装置实施 QoS 要求 RQ 的进一步鉴权。为此譬如通过标准化的协议 COPS 发送查询到资源控制器 RC 上。该资源控制器 RC 控制，在通信网中可否提供所要求的 QoS。资源控制器 RC 为此仅须知道通信网中的整个存在的（或已占用的）资源，以便可以对 COPS 查询发送应答。由关守 CC_{GK} 已经查明使用者对于通话 CALL 本身的特许。在该变型方案中，在资源控制器 RC 和关守 CC_{GK} 之间，以及在资源控制器 RC 和（使用者）数据库 DB 之间不需要接口和消息。

[0094] 边缘装置 PER_A 在接收资源控制器 RC 的应答之后如下来作出反应：要么由于通信网中的过负荷，或由于在考虑令牌 T 的条件下的不成功的验证而拒绝 QoS 要求 RQ，要么在通信网中从配置上来调节所要求的 QoS，譬如通过动态激活策略、或替代于在边缘装置 PER_A 中的 RSVP 终止而通过将 RSVP 预留经由网络传输到另一个边缘装置 PER_B 或端点 B 为止。但是这对于在这里所介绍的解决办法是不重要的。

[0095] 在从边缘装置 PER_A 收到肯定的 RSVP 应答之后，端点 A 开始信息传输。在此，譬如按实时控制协议 (RTCP) 传输信令数据，并譬如按实时协议 (RTP) 传输媒体数据。在通话 CALL 持续期间，现在专门针对该通话 CALL 和使用者按使用者的特许以及 ISP 的网络中的负荷情况来确保 QoS。

[0096] 为了进一步提高安全性，重复给端点 A 传输改变的令牌 T。这譬如以少数几秒的有规则的间隔来实现。在此，如果可以将同样存在着的消息用于传输这些令牌 T，则产出特别良好的优点。譬如在通话 CALL 期间，端点 A 和关守 CC_{GK} 可以通过有规则交换的“保持激活”消息而处于持续的通信连接之中（对此请参阅 H.225.0(02/98)，章节 7.9.1 和 7.9.2，在消息注册确认 RCF 中用于设置注册寿命的参数“寿命”(timeToLive)，以及在消息注册请求 RRQ 中用于刷新、即延长已有注册寿命的参数“保持激活”(keepAlive))。这些“保持激活”消息的周期通常是有规则的，并位于秒的范围中。在这些消息中可以随同发送重新加密编码的令牌 T，使得端点 A 获得供支配的、用于在通信网中刷新″软″预留的重复加密编码的令牌 T。

[0097] 通过将其值可变化的信息、譬如随机数和 / 或时标集成到加密编码的令牌 T 中，来达到特别高的安全性。在此，也可以有利地用同一个机密 K 来加密编码和解密译码每个刷新消息。如果将一个时标插入已加密编码的 QoS 要求 RQ 中，则另外还保证了端点 A 不能延迟或存储令牌 T，以便在稍后的时刻来转送它。因此排除了，在夜间适用低费率时聚集、而在白天高费率时才采用加密编码的令牌 T。

[0098] 通过从终端设备 A 出发的消息 RELEASE（释放）来显示通话 CALL 的结束。作为后果，关守 CC_{GK} 停止将加密编码的令牌 T 发送到端点 A 上，并终止所述通话 CALL 的选择地开始的计费。边缘装置 PER_A 因而也没有得到其它的加密编码的令牌 T，使得在短时间后取消了通信网中的预留。于是资源控制器 RC 可以重新分配空出来的资源。

[0099] 通过信令将通话 CALL 的结束也通知给端点 B 的呼叫控制器 CC_{SIP}。该呼叫控制器 CC_{SIP} 同样仃止发送加密编码的令牌 T_B。所有由端点 B 在通信网中对于通话 CALL 所采取的预留也因而失效。因此一致地释放通话 CALL。

[0100] 譬如按在 ITU 标准 H.235v2，″ H 系列（基于 H.323 和其它 H.245 的）多媒体终

端的安全性和加密″，2000，附件 D-F 中所说明的分散机制中的一个或其组合来实现令牌 T 的加密编码和解密译码，这些分散机制用于保证（譬如按 ITU 标准 H.225.0 构成的）信息传输：

[0101] －具有按 H.235，附件 D 的对称机密的鉴权和完整性：由发送器借助机密来形成关于整个（信令）消息的、构成为密码散列值的签名，并在传输时附加在消息上。由接收器借助相同的机密将所述的散列值译码。如果所述的散列值在译码之后与所述消息相称，则发送器被可靠地识别。机密被构成为通行字，并被存放在中央服务器中。在发送器和接收器中在带外管理它们。

[0102] －具有按 H.235，附件 E 的非对称机密的鉴权和完整性：由发送器形成关于整个（信令）消息的密码数字式签名。此外，还应用在带内传输或在带外管理的证书。在终端设备中手动管理专用的密钥。签名当今还是一种费事的计算操作，该计算操作由于实时要求不适合于应用在任何信息传输上。但是随着计算系统效率的不断提高，该边界条件应越来越退居次要的地位。

[0103] －具有按 H.235，附件 F 的混合机密的信令的鉴权和完整性：实现以上两个方法的组合，其中，借助 Diffie-Hellman 法附加地交换所谓的会话密钥。此时，在每个方向上数字式地签名第一消息，所有其它的消息对称地受到完整性保护。此外，在带内传输或在带外管理的证书还得到采用。

[0104] －具有按照语音加密简要表 (VEP) 的、按 H.235，附件 D 的对称机密的媒体数据的保密性：此时，在终端设备之间借助已鉴权的 Diffie-Hellman 法商定一个用于加密编码媒体数据的独立的共同密钥。

[0105] 如果借助已经存在的、在本实施例中按 H.323 标准族或 RSVP 协议构成的消息来实施本发明的方法步骤，则得出特别良好的优点，譬如其方式是将与本发明有关的信息插入已经存在的、必要时专门的消息阵列中，在有关的标准中安排了这些消息阵列譬如作为没有功能说明（可选的参数）的空白阵列。

[0106] 譬如终端设备将加密编码的令牌 T 插入一个到资源控制层 RCL 上的否则未改变的 RSVP 预留消息 RQ_{RSVP} 中。为此可以考虑譬如 RSVP 的零对象 (NULL Objekt)。IETF 标准 RFC2205 如下来说明该元素：″零对象具有零的类号，而它的 c 类型是被忽略的。它的长度必须最少为 4，但可以是 4 的任意倍数。零对象可能出现在对象序列中的任何地方，而它的内容将被接收器忽略″。

[0107] 替代地，将加密编码的令牌 T 譬如插入标准化的 RSVP 消息的阵列 INTEGRITY（完整性）中。按 IETF 标准 RFC2205 该阵列载有如下的信息：″载有密码数据用于鉴权始发节点和验证该 RSVP 消息的内容″。说明″始发节点″（＝使用者终端设备，端点）在此未给出由呼叫控制层 CCL 提供加密编码令牌 T 的提示。更确切地说，在这里考虑到了在自主的端点 A，B 和资源控制层 RCL 之间所商定的加密编码。

[0108] 用于传输与本发明有关的信息的独立的信息当然也是可能的。作为其它的替代方案也可以手动配置两个机密 K_A，K_B。在以降低装置的灵活性为代价的情况下，在终端设备 A，B 注册时由此免去采用费事的 Diffie-Hellman 法，这在相应固定配置的通信网中可能完全是合理的和受欢迎的。附图 3 中示出了所述方法的一个相应的扩展方案。在此，在终端设备 A，B 和中央级 C 中手动预配置了机密 K_A，K_B。可靠地通过机密 K_A，K_B 传输有关注册和呼

叫建立的信令。

[0109] 最后要强调，通信网的对本发明重要的部件的说明原则上不应理解为限制性的。对于有关的专业人员尤其显然的是，应将象‘端点’、‘呼叫控制层’、或‘资源控制层’那样的概念理解为功能性的而不是物理的。因此譬如也可以部分或完全地以软件和/或在多个物理的装置上分布式地来实现所述的端点 A，B。

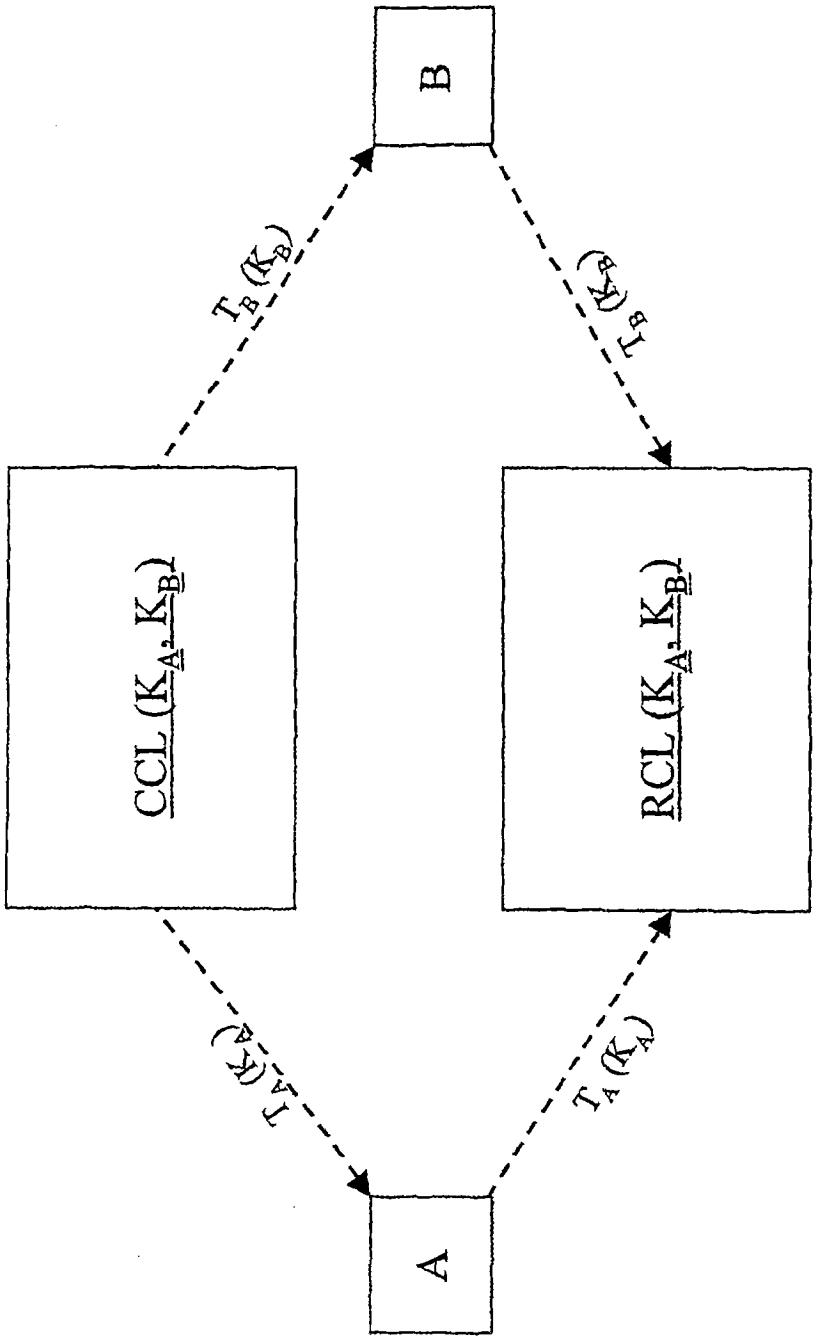


图 1

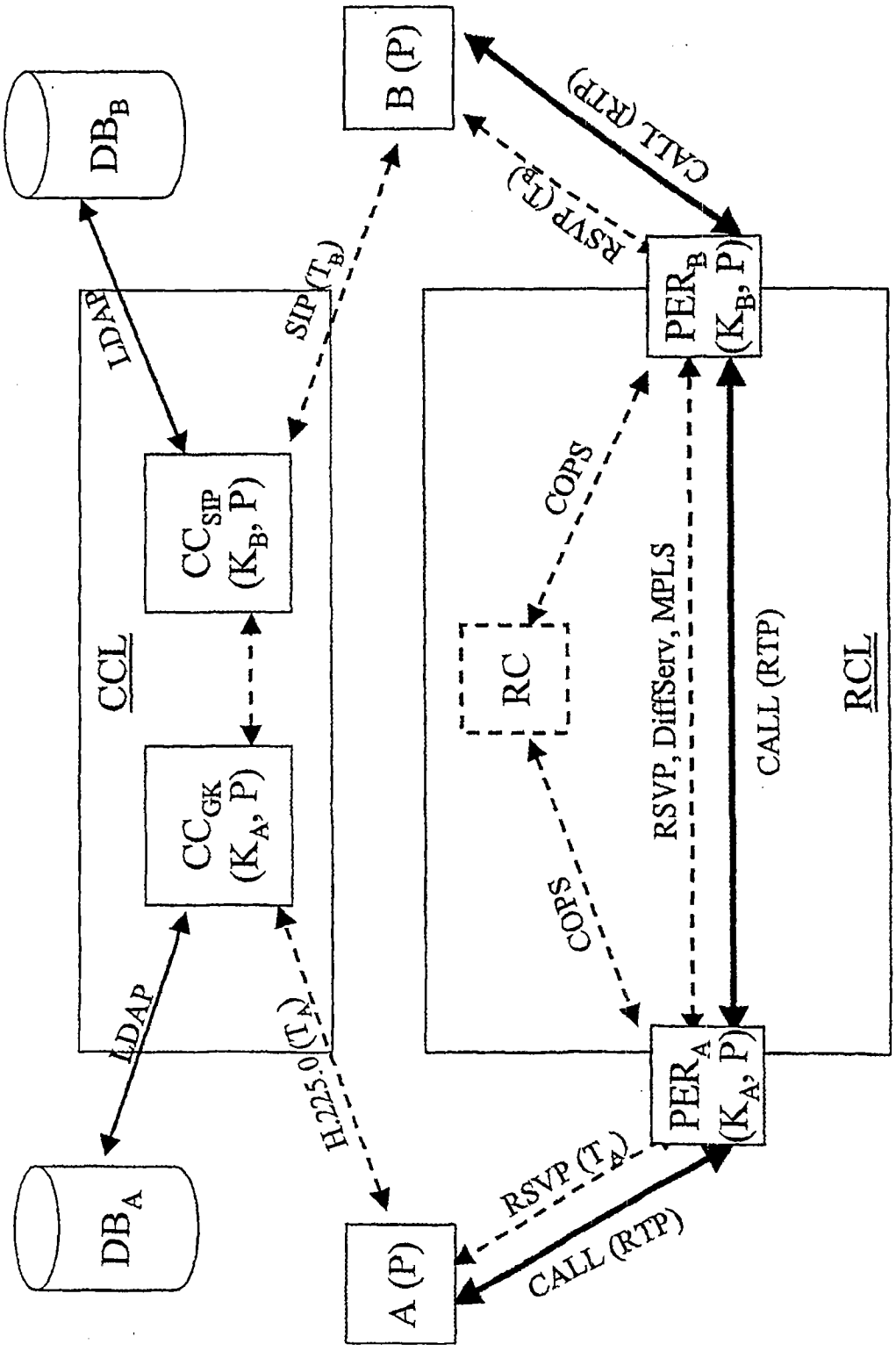

B (P)
CALL (RTP)
RSVP (T_B)
DB_B
LDAP
SIP (T_B)
PER_B (K_B, P)
CC_SIP (K_B, P)
CCL
COPS
RC
RSVP, DiffServ, MPLS
CALL (RTP)
RCL
CC_GK (K_A, P)
COPS
LDAP
H.225.0 (T_A)
PER_A (K_A, P)
DB_A
RSVP (T_A)
CALL (RTP)
A (P)

图 2

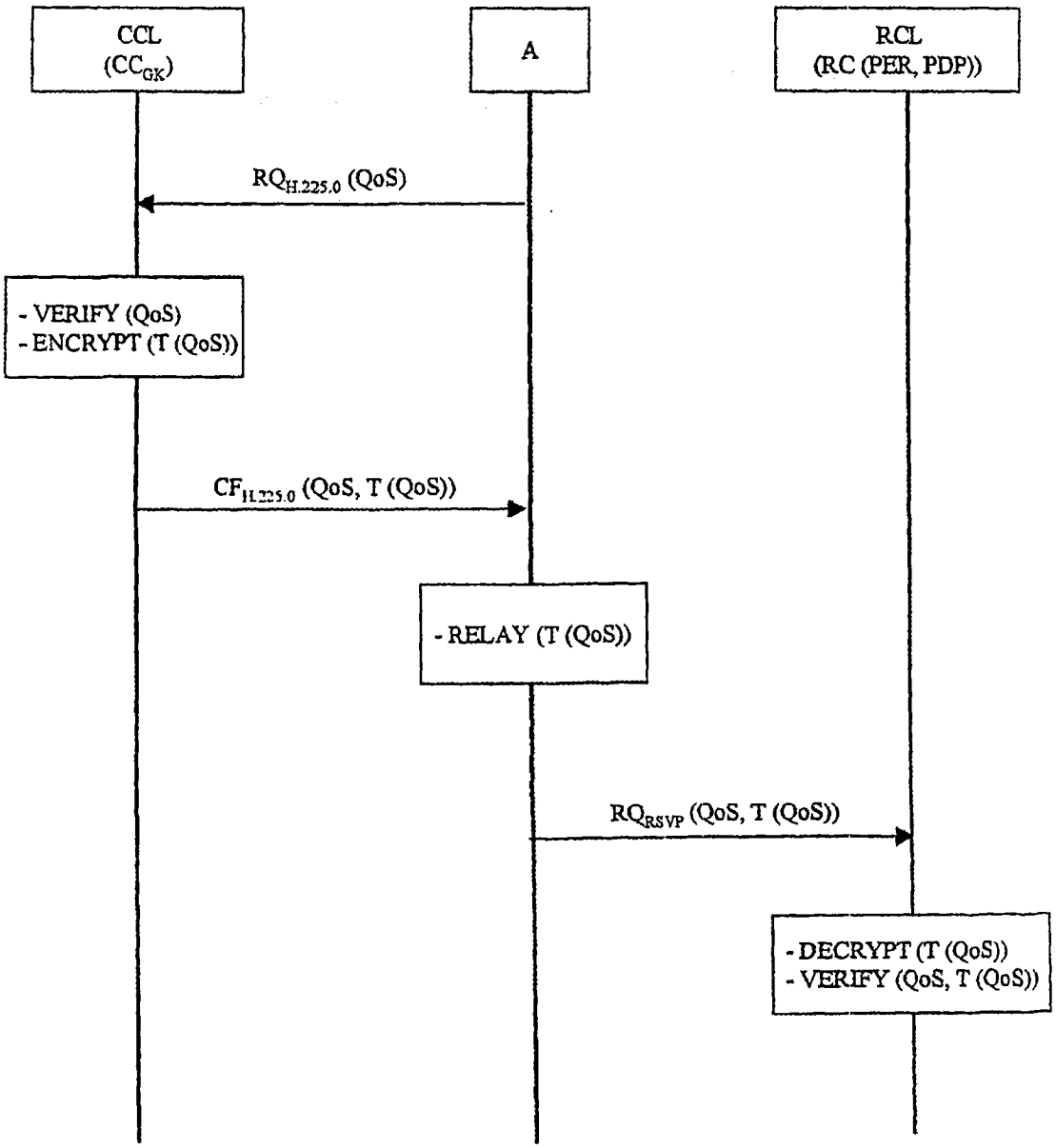

CCL
(CC_GK)
A
RCL
(RC (PER, PDP))
RQ_H.225.0 (QoS)
- VERIFY (QoS)
- ENCRYPT (T (QoS))
CF_H.225.0 (QoS, T (QoS))
- RELAY (T (QoS))
RQ_RSVP (QoS, T (QoS))
- DECRYPT (T (QoS))
- VERIFY (QoS, T (QoS))

图 3