



(12) 发明专利申请

(10) 申请公布号 CN 104303198 A

(43) 申请公布日 2015.01.21

(21) 申请号 201380000191.5

代理人 魏小薇

(22) 申请日 2013.04.22

(51) Int. Cl.

(30) 优先权数据

G06Q 20/38(2006.01)

1353407 2013.04.15 FR

G06Q 20/20(2006.01)

(85) PCT国际申请进入国家阶段日

2013.04.28

(86) PCT国际申请的申请数据

PCT/FR2013/050888 2013.04.22

(87) PCT国际申请的公布数据

W02014/170561 FR 2014.10.23

(71) 申请人 阔达银行

地址 法国克鲁瓦

(72) 发明人 B·费兰 A·里泽

(74) 专利代理机构 中国国际贸易促进委员会专  
利商标事务所 11038

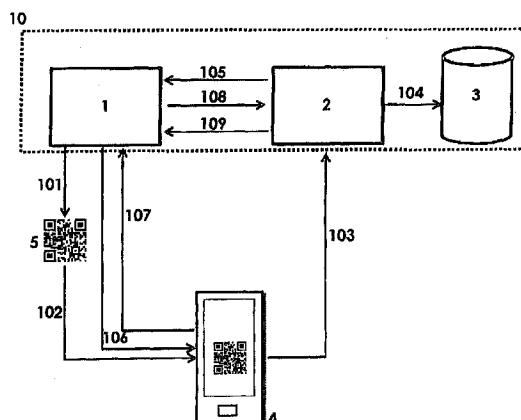
权利要求书2页 说明书7页 附图1页

(54) 发明名称

提高电子交易安全性的方法与系统

(57) 摘要

通过服务器(2)和销售终端(1)分别构建第一和第二加密消息；通过销售终端(1)通过使用第二加密消息构建第三加密消息，而后将其传送至服务器(2)；通过服务器(2)使用第一加密消息解密第三加密消息；通过服务器(2)根据解密的第三信息的内容、通过使用第一加密消息构建第四加密消息，而后将其传送至销售终端(1)；通过销售终端(1)使用第二加密消息解密第四加密消息。销售终端1生成并显示与例如QR码5的形式的交易相关的一组信息。该标识信息然后将被由销售终端1生成的包含一组随机字符的随机串补充。解密密钥是通过使用两个随机数生成的。



1. 一种在销售终端 (1) 和交易控制服务器 (2) 之间进行安全通信的方法, 所述方法包括 :

- 由交易控制服务器 (2) 根据第一加密算法基于至少一个第一数据来构建第一加密消息;

- 由销售终端 (1) 根据相同的第一加密算法基于假定与所述第一数据相同的至少一个第二数据来构建第二加密消息;

该方法的特征在于还包括 :

- 由所述销售终端 (1) 根据第二加密算法、通过把所述第二加密消息用作加密密钥、基于至少一个第三数据来构建第三加密消息;

- 由所述销售终端 (1) 把所述第三加密消息传送到所述交易控制服务器 (2);

- 由所述交易控制服务器 (2) 根据所述第二加密算法、通过把所述第一加密消息用作解密密钥来对所述第三加密消息进行解密;

- 由所述交易控制服务器 (2) 根据第三加密算法、通过把所述第一加密消息用作加密密钥、根据解密的所述第三消息的内容来构建第四加密消息;

- 由所述交易控制服务器 (2) 把所述第四加密消息传送至所述销售终端 (1);

- 由所述销售终端 (1) 根据所述第三加密算法、通过把所述第二加密消息用作解密密钥来对所述第四加密消息进行解密。

2. 根据权利要求 1 所述的方法, 还包括由所述销售终端 (1)、根据解密的所述第四消息来准许交易或终止交易的步骤。

3. 根据权利要求 1 或 2 所述的方法, 其中, 所述第三数据包括随机串, 该随机串在销售终端 (1) 和交易控制服务器 (2) 已知的一些位置上含有销售终端 (1) 和交易控制服务器 (2) 预先约定的信息。

4. 根据权利要求 1 或 3 所述的方法, 其中, 所述第四加密消息的构建包括对随机串的加密, 该随机串在销售终端 (1) 和交易控制服务器 (2) 已知的一些位置上含有交易的返回码。

5. 根据权利要求 4 所述的方法, 其中, 所述返回码在构建时被检验字节补充。

6. 根据权利要求 1 至 5 中任一项所述的方法, 其中, 所述第一数据和所述第二数据对应于用户密码。

7. 根据权利要求 1 至 6 中任一项所述的方法, 其中, 所述第一数据和所述第二数据包括相同的随机串。

8. 一种交易控制服务器 (2), 被配置为 :

- 根据第一加密算法、基于至少一个第一数据来构建第一加密消息;

- 接收第二加密消息;

- 根据第二加密算法、通过把所述第一加密消息用作解密密钥来对所述第三加密消息进行解密;

- 使用所述第一加密消息作为加密密钥来根据解密的所述第二消息的内容、按照第三加密算法来构建第三加密消息;

- 传送所述第三加密消息。

9. 一种销售终端 (1), 被配置为 :

- 根据第一加密算法、基于至少一个第一数据来构建第一加密消息;

- 使用所述第一加密消息作为加密密钥来根据第二加密算法基于至少一个第二数据构建第二加密消息；

- 传送所述第二加密消息；

- 接收第三加密消息；

- 根据第三加密算法、通过把所述第一加密消息用作解密密钥来对所述第三加密消息进行解密；

- 根据解密的所述第三消息来准许交易或者终止交易。

10. 一种在销售终端 (1) 和交易控制服务器 (2) 之间进行安全通信的系统，所述系统包括：

- 交易控制服务器 (2)，被配置为根据第一加密算法基于至少一个第一数据来构建第一加密消息；

- 销售终端 (1)，被配置为根据相同的第一加密算法基于假定与所述第一数据相同的至少一个第二数据来构建第二加密消息；

该系统的特征在于还包括：

- 被配置为根据第二加密算法、通过把所述第二加密消息用作加密密钥、基于至少一个第三数据来构建第三加密消息的销售终端 (1)；

- 被配置为把所述第三加密消息传送到所述交易控制服务器 (2) 的销售终端 (1)；

- 被配置为根据所述第二加密算法、通过把所述第一加密消息用作解密密钥来对所述第三加密消息进行解密的交易控制服务器 (2)；

- 被配置为根据第三加密算法、通过把所述第一加密消息用作加密密钥、根据所述第三加密消息的内容来构建第四加密消息的交易控制服务器 (2)；

- 被配置为把所述第四加密消息传送至所述销售终端 (1) 的交易控制服务器 (2)；

- 被配置为根据所述第三加密算法、通过把所述第二加密消息用作解密密钥来对所述第四加密消息进行解密的销售终端 (1)。

11. 根据权利要求 10 所述的系统，其中，销售终端 (1) 还被配置为实施根据解密的所述第四消息来批准交易或终止交易的步骤。

12. 一种在存储介质上实施的计算机程序产品，能够用在计算机处理单元中并且包括用于实施根据权利要求 1 至 7 之一的方法的指令。

## 提高电子交易安全性的方法与系统

- [0001] 本发明涉及销售终端与交易控制服务器之间的通信安全的技术领域。
- [0002] 下文中“销售终端”指的是任何可以进行电子交易的物理设备或虚拟设备。非穷举地可以列举：
- [0003] - 如物理销售终端：针对运输领域（铁路、航空、航海）的参与者的交通票售卖端、商业网点（药店、餐馆）的收款机、在某些商店（超市）中配备有“自助结帐”系统的收款台；
- [0004] - 如虚拟销售终端：通过网页站点和 / 或专用移动应用来提供销售服务和 / 或产品的电子商务网点。
- [0005] 为了能够确保交易，销售终端的管理人员要在销售点布置所述终端。
- [0006] 这里的“销售点”(POS, Point of Sale) 指的是提议完成交易、特别是销售产品（例如农产品、药品、多媒体设备）和 / 或出售服务（例如送货、餐饮、旅游、旅馆）的任何物理或虚拟场所，不管是何种规模或属于哪种经营范围。
- [0007] 根据用户销售终端上发起的交易请求，可以使该销售终端进行许多任务以完成此次交易。这些任务尤其包括识别和记录要向用户开价的商品（产品和 / 或服务）、告知与所述交易相关的用户、并最后管理支付事宜。
- [0008] 告知与所述交易相关的用户的任务包括例如向用户提供标识交易的号码、标识用户所使用的销售终端的号码、交易涉及的产品和 / 或服务的列表摘要、向用户开具的总金额或者交易状态。
- [0009] 交易所涉及的信息总和可以根据不同的方式显示出来：或者是以虚拟方式例如通过支付端的显示屏显示，或者是以实体方式在如收银小票之类的载体上显示。
- [0010] 不管是以哪一种方式（实体或虚拟的）显示交易相关的信息，所述信息可以采用不同的方法显示：例如文本形式、条形码、标签、QR 码（“快速反应”码）、通过 NFC 类型信号、或更一般地所有类型的信息编码。
- [0011] 此外，为了保证用户使用销售终端的舒适性及由此带来的高满意度，所述销售终端必须能够保证最新技术的支持。在这些最新技术中，可以特别列举来自于用户的移动终端和 / 或安装在用户移动终端上的移动应用的支付媒介，以便优选地通过无线界面与销售终端进行交互。
- [0012] 所谓“移动终端”，这里指的是移动电话、智能手机、PDA（“个人数字助理”）或任何其它类型的能够收集由销售终端打印或显示的交易信息并能够与远程服务器进行交互的通信系统。
- [0013] 例如，通过移动终端的停车远程支付服务，经不同的销售终端向不同类别的终端用户提供支付服务。要支付停车票的驾驶人员选择由在实时计时器或互联网上显示的代码表示的停车区域或停车价格，随后确认车辆以及希望的时段。这种方案可以在任何类型的便携式电话上实现。这样，可以通过互联网浏览器、甚至是专门的智能手机应用就可以访问业务。
- [0014] 图 1 显示了销售系统 10，包括销售终端 1 和远程交易控制服务器 2。

[0015] “交易控制”是指对与交易相关联的所传送的信息（例如识别码、编码、交易状态）列表的管理（例如接收、检验、准许、验证）。

[0016] 在现有技术中，要在销售终端和具有移动终端的用户之间进行交易而实施的方法如下。

[0017] 在具有移动终端4（例如智能手机）的用户执行的交易请求后，销售终端1生成并显示与该项交易相关的全部信息（交互101），例如为QR码5的形式。

[0018] 借助于智能手机4，用户通过专门的应用获取所述QR码5（交互102）。

[0019] “专门的应用”指的是由用户安装并且符合特定服务的需求的应用。用户在可以使用相应的专门的应用之前可以事先预订所述特定服务。因此例如，在与支付服务相关的情况下，用户需要事先预订所述服务并提供与之相关的某些个人数据，例如用户的银行标识码。在用户预订了支付服务之后，专门的应用便在用户的智能手机里存储了与用户支付卡相关联的加密密匙以及与用户密码相关联的加密密匙，用于以后在交易时使用。

[0020] 这里所说的智能手机的使用以及用于获取QR码的专门的应用为非限制性的示例，并且通常涉及由配有适当设备的任何移动终端所进行的交易信息的获取。

[0021] 一旦QR码被获取，智能手机4向远程交易控制服务器2传送：所获取的QR码，标识元素（例如智能手机和/或用户的标识码）、用户支付卡的解密密匙、以及用户密码的解密密匙（交互103）。

[0022] 接收到这些数据后，交易控制服务器2借助QR码来识别销售终端1。然后，该交易控制服务器创建交易识别码并在数据库3中插入记录（交互104），包括与交易相关的元素（例如智能手机4的识别码和销售终端1的识别码）以及与交易状态相关的代码。

[0023] 借助交互103时传送的相应的解密密匙，交易控制服务器2然后对用户卡的数据进行解密，然后发起负责查探与交易状态相关的代码的存储处理以便到时候启动交易准许请求。

[0024] 而后，交易控制服务器2借助交互103时传送的相应的解密密匙来对用户的密码进行解密，并生成第一随机串。所述第一随机串然后与用户密码级联，然后根据第一加密算法进行加密。最终可以获得名为“CSC”（安全加密码）的加密数据串。所获得的CSC串（第一加密消息）然后在交易（交互104）处被存储在数据库3中。

[0025] 所述第一随机串随后被交易控制服务器2传送到负责与用户进行交易的销售终端1（交互105）。

[0026] 接收到第一随机串时，销售终端1邀请用户输入密码（交互106）。该密码：

[0027] - 或者假定与通过交易控制服务器2解密的所述密码相同；

[0028] - 或者更一般地与通过交易控制服务器2解密的密码相关，也就是说，通过运行特定的方法由另一密码推导得出。

[0029] 获取并验证用户的密码后（交互107），销售终端1把所输入的密码与通过交互105传送的所述第一随机串级联，而后应用同类型的加密，也就是说，使用与交易控制服务器2相同的第一加密算法，以便生成下文将用“输入的CSC”表示的CSC串（第二加密消息）。

[0030] 交互108允许销售终端1把“输入的CSC”传送至交易控制服务器2。

[0031] 假定传送到销售终端1的用户密码与交易控制服务器2处解码的第一密码相同（或相关），因此所得到的“输入的CSC”被假定与交易控制服务器2生成的CSC相同。

[0032] 接收到“输入的 CSC”后，交易控制服务器 2 将“输入的 CSC”与它自己生成并存储在数据库 3 中的 CSC 相比较。如果这二者一致，则所传送的用户密码是正确的并且交易控制服务器 2 执行准许并通过交互 109 告知销售终端 1 其可以结束交易。在相反的情况下，交易控制服务器通过交互 109 告知销售终端 1 用户输入的密码错误以便请用户再次输入其密码（交互 106 和 107）并且因此将新的“输入的 CSC”重新传送至交易控制服务器 2（交互 108）。

[0033] 该方法的优点主要在于所输入的同一个密码在两次不同的交易中给出两个不同的加密串（“输入的 CSC”）。这样可以确保无法得到用户的密码。

[0034] 然而，该方法的过程中被证实有重要缺点，从而使之容易受到已知通常称之为“中间人”的攻击。“中间人”攻击尤其包括查探 / 拦截交易控制服务器 2 与销售终端 1 之间的交互（交互 105、108 和 109）而后经由交互 109、通过系统性地向销售终端 1 做出成功（或失败）的应答来模拟交易控制服务器 2，不管通过交互 108 传送的“输入的 CSC”正确与否。

[0035] 交互 109 尤为关键，因为其传送交易控制服务器 2 的最终应答：也就是说，根据该交互 109 传送出的应答，销售终端 1 验证通过 / 拒绝和 / 或终止此次交易。因此现有技术的各种局限之一就在于交互 109 已被证实的易受攻击性，特别是在该交互过程中使用的协议可以被外部个体分析和复制的情况下。

[0036] 另一缺点允许已知名为“暴力攻击”的攻击对交互 108 进行处理。该处理包括通过穷举的方式将字符的所有可能的组合进行测试，以得到至少一个有效信息，在这里即为用户的密码。

[0037] 这样，如果黑客掌握了销售终端 1 使用的加密算法并能够拦截交互 108，他便可以通过“暴力攻击”手段在“输入的 CSC”中识别用户的密码。

[0038] 本发明的一个目的是克服现有技术中的这些缺点。

[0039] 本发明的另一个目的是能够改进销售终端和交易控制服务器之间的交换的安全性。

[0040] 为此，根据其第一方面，本发明涉及在销售终端和交易控制服务器之间进行安全通信的方法，所述方法包括：

[0041] - 由交易控制服务器根据第一加密算法基于至少一个第一数据来构建第一加密消息；

[0042] - 由销售终端根据相同的第一加密算法基于假定与所述第一数据相同的至少一个第二数据来构建第二加密消息；

[0043] 该方法还包括：

[0044] - 由所述销售终端根据第二加密算法、通过把所述第二加密消息用作加密密钥、基于至少一个第三数据来构建第三加密消息；

[0045] - 由所述销售终端把所述第三加密消息传送到所述交易控制服务器；

[0046] - 由所述交易控制服务器根据所述第二加密算法、通过把所述第一加密消息用作解密密钥来对所述第三加密消息进行解密；

[0047] - 由所述交易控制服务器根据第三加密算法、通过把所述第一加密消息用作加密密钥、根据解密的所述第三消息的内容来构建第四加密消息；

[0048] - 由所述交易控制服务器把所述第四加密消息传送至所述销售终端；

[0049] - 由所述销售终端根据所述第三加密算法、通过把所述第二加密消息用作解密密钥来对所述第四加密消息进行解密。

[0050] 根据第二方面，本发明涉及交易控制服务器，其被配置为：

[0051] - 根据第一加密算法、基于至少一个第一数据来构建第一加密消息；

[0052] - 接收第二加密消息；

[0053] - 根据第二加密算法、通过把所述第一加密消息用作解密密钥来对所述第二加密消息进行解密；

[0054] - 使用所述第一加密消息作为加密密钥来根据解密的所述第二消息的内容、按照第三加密算法来构建第三加密消息；

[0055] - 传送所述第三加密消息。

[0056] 根据其第三方面，本发明涉及销售终端，其被配置为：

[0057] - 根据第一加密算法、基于至少一个第一数据来构建第一加密消息；

[0058] - 使用所述第一加密消息作为加密密钥来根据第二加密算法基于至少一个第二数据构建第二加密消息；

[0059] - 传送所述第二加密消息；

[0060] - 接收第三加密消息；

[0061] - 根据第三加密算法、通过把所述第一加密消息用作解密密钥来对所述第三加密消息进行解密；

[0062] - 根据解密的所述第三消息来准许交易或者终止交易。

[0063] 根据第四方面，本发明涉及在销售终端与交易控制服务器之间进行安全通信的系统，所述系统包括：

[0064] - 交易控制服务器，被配置为根据第一加密算法基于至少一个第一数据来构建第一加密消息；

[0065] - 销售终端，被配置为根据相同的第一加密算法基于假定与所述第一数据相同的至少一个第二数据来构建第二加密消息；

[0066] 该系统还包括：

[0067] - 被配置为根据第二加密算法、通过把所述第二加密消息用作加密密钥、基于至少一个第三数据来构建第三加密消息的销售终端；

[0068] - 被配置为把所述第三加密消息传送到所述交易控制服务器的销售终端；

[0069] - 被配置为根据所述第二加密算法、通过把所述第一加密消息用作解密密钥来对所述第三加密消息进行解密的交易控制服务器；

[0070] - 被配置为根据第三加密算法、通过把所述第一加密消息用作加密密钥、根据所述第三加密消息的内容来构建第四加密消息的交易控制服务器；

[0071] - 被配置为把所述第四加密消息传送至所述销售终端的交易控制服务器；

[0072] - 被配置为根据所述第三加密算法、通过把所述第二加密消息用作解密密钥来对所述第四加密消息进行解密的销售终端。

[0073] 根据其第五方面，本发明涉及在存储介质上实施的计算机程序产品，能用于计算机处理单元中并且包括用于实施以上所概述的方法的指令。

[0074] 参照以示意图形式描述实施方式背景的附图 1，通过阅读以下说明书中的优选实

施方式,本发明的其它特征和优点变得更清楚、更具体。

[0075] 本发明提出使通过交互 101、102、103 传送的 QR 码 5 的内容更加丰富并且修改通过交互 108 和 109 传送的交换内容。

[0076] 当持有移动终端 4(例如智能手机)的用户提出交易请求后,销售终端 1 生成并以例如 QR 码 5 的形式显示出与该交易相关的一组信息(交互 101)。

[0077] 生成然后显示的该组信息包括与交易相关的信息,其中至少有由销售终端 1 提供的识别信息。

[0078] 通常,由销售终端 1 提供的识别信息包括销售终端 1 与交易控制服务器 2 之间预先约定的所有信息,或者还包括两边都已知的任何其它信息。

[0079] 例如,由销售终端 1 提供的识别信息可以包括为交易控制服务器 2 所知的认证令牌和 / 或 IP 地址。

[0080] 该识别信息随后将被由销售终端 1 生成的、由一系列随机字符组成的随机串补充。

[0081] 以下将该随机串称为“第二随机串”,以便区别于在构建第一加密消息 CSC 时在交易控制服务器 2 处生成的第一随机串。

[0082] 在一个实施方式中,销售终端 1 生成并以例如 QR 码 5 的形式显示了一组信息(交互 101),该组信息由交易控制服务器 2 所知的认证令牌构成,所述认证令牌被由销售终端 1 生成的一系列随机字符补充。

[0083] 由销售终端 1 显示(交互 101)、被移动终端 4 获取(交互 102)并被传送到交易控制服务器 2(交互 103)的 QR 码 5、更一般地是该组信息,因此发现其内容由于销售终端 1 添加的第二随机串的存在而被丰富。

[0084] 接收 QR 码 5 后,交易控制服务器 2 将 QR 码 5 分成两部分:

[0085] - 含有补充信息的部分,这里指的是用于识别销售终端的认证令牌;

[0086] - 含有由销售终端 1 添加的第二随机串的部分。

[0087] 交易控制服务器 2 构建第一加密消息包括:

[0088] - 通过交易控制服务器 2 生成第一随机串;

[0089] - 将解密的用户密码与所述第一随机串级联;

[0090] - 使用第一加密算法来对所级联的第一随机串和密码进行加密。

[0091] 在一实施方式中,含有所述第二随机串的 QR 码 5 的那一部分,允许对所述第一加密消息的构建进行补充:

[0092] 由交易控制服务器 2 生成的所述第一随机串与用户密码级联,随后与 QR 码 5 中所含有的所述第二随机串级联。所获得的串最后根据第一加密算法被加密。这样便获取了与 CSC 相对应的第一加密消息。

[0093] 同样,输入并验证用户密码(交互 107)后,销售终端 1 将输入的密码与由交互 105 传送的所述第一随机串进行级联,然后再与销售终端 1 生成的第二随机串级联。随后运用相同的加密方式,也就是说,使用与交易控制服务器 2 相同的所述第一加密算法,以生成与“输入的 CSC”相对应的第二加密消息。

[0094] 使用第二随机串用以构建 CSC 和“输入的 CSC”(分别为第一和第二加密消息)的优点在于这些消息的复杂性。更具体地,从技术效果来说,这允许加大这些消息的平均信息

量 (entropie) :对交互 108 要进行“暴力”型攻击所进行测试的组合的数目就会变得极其大。这样,即使黑客掌握了用于构建这些消息的加密算法,考虑到所需测试的组合数目,这两个随机串的存在使得实施这一方法变得几乎不可能实现。

[0095] 可注意到另外一个优点是,与由交互 105 传送的第一随机串相反,第二随机串并非直接在交易控制服务 2 与销售终端 1 之间传输。这样,即使黑客能够拦截含有第一随机串的交互 105,并且掌握销售终端 1 所使用的加密算法,第二随机串的存在也将限制“暴力”型攻击的风险。

[0096] 所述“输入的 CSC”然后被利用作为第二加密算法过程中的加密密钥以便构建新的消息(第三加密消息)。所述第三加密消息由包含销售终端 1 的识别码的随机串组成,该识别码位于销售终端 1 与交易控制服务器 2 已知的随机串中的特定位置处。

[0097] 由销售终端 1 构建的所述第三加密消息随后被传送至交易控制服务器 2(交互 108)。

[0098] 接收到所述第三消息后,交易控制服务器 2 基于相同的所述第二加密算法把已经存储在数据库 3 中的 CSC 作为解密密钥,以便通过使用销售终端识别码的位置的知识来解密收到的消息。如果销售终端 1 的识别码在解密的信息中被找到,则在交互 107 中用户输入并传送的密码是正确的。相反,如果销售终端 1 的识别码没有在解密的信息中被找到,这意味着“输入的 CSC”不同于数据库 3 中存储的 CSC,因而用户所输入的密码不正确。

[0099] 需注意的是使用销售终端 1 的识别码来构建第三加密消息、所述识别码的位置、及其在第三加密消息解密时的重新识别是非限制性的示例。一般地,可以使用销售终端 1 与交易控制服务器 2 事先约定的其它任何信息,或是双方已知的其它任何信息。可以列举其它信息,例如,销售终端 1 的 IP 地址。

[0100] 然后,交易控制服务器 2 根据所解密的消息的内容来生成检验消息。所述检验消息由一个随机串构成,在该随机串中交易控制服务器 2 在销售终端 1 和其自身所知的一些位置上放置交易指令码,这里指交易的“返回码”。该“返回码”是例如与交易状态相关联的编码消息:如果交易被验证有效的话为“OK”,或反之为“KO”。

[0101] 所述检验消息随后借助存储于数据库 3 中的 CSC、根据第三加密算法进行加密(获得第四加密消息),而后通过交互 109 传送至销售点。

[0102] 接收所述第四加密消息时,销售点 1 基于相同的所述第三加密算法,使用“输入的 CSC”作为解密密钥来解密所述第四加密消息。被解密的所述消息因此与所述验证信息相对应。销售点然后使用所述“返回码”的位置的知识,从所述验证信息中提取交易的“返回码”。

[0103] 如果提取的该“返回码”被销售终端 1 判断为一致,这意味着用户输入的密码是正确的。然后根据所述“返回码”的内容来进行交易的准许和 / 或终止。例如可以检验“返回码”中的与交易的“OK”状态或“KO”状态相关联的编码消息的存在。

[0104] 反之,用户会被再次要求输入密码(交互 106 和 107)以便重新发送。

[0105] 此外,当用户密码输入出错时,“输入的 CSC”能够允许对难证信息(通过交互 109 传送)解密以便从中提取一致的“返回码”的可能性取决于要被检验的信息的长度。

[0106] 作为要检验的信息的例子,可以列举所述检验消息中存在的交易的“返回码”的长度。

[0107] 因此,在一种实施方式中,可以约定构建足够长的“返回码”,以便在用户的密码出错时,使提取出一致的“返回码”的可能性趋于零。

[0108] 有利地,可以在构建时通过 CRC32 类型的控制字节对该“返回码”进行补充。

[0109] 有利地,收听到销售终端 1 与交易控制服务器 2 之间交换的信息的入侵者无法通过交互 109 来构建告知销售终端 1 可以顺利(或不顺利)结束交易的消息。

[0110] 本发明的另一优点是同一销售终端 1 上输入的两个相同代码导致在同一交易中构建两条不同的消息,因此入侵者无法分析所使用的协议。

[0111] 有利地,以上描述的方法允许:

[0112] - 改进电子交易的安全性;

[0113] - 加强交易控制服务器与销售终端之间进行的交换的安全性;

[0114] - 改进交易控制服务器与销售终端之间的交换的内容,而无需分别改变相应的交互;

[0115] - 阻止对所使用协议的任何外部分析;

[0116] - 阻止任何“暴力”型攻击;

[0117] - 限制受到“中间人”类型攻击的任何风险。

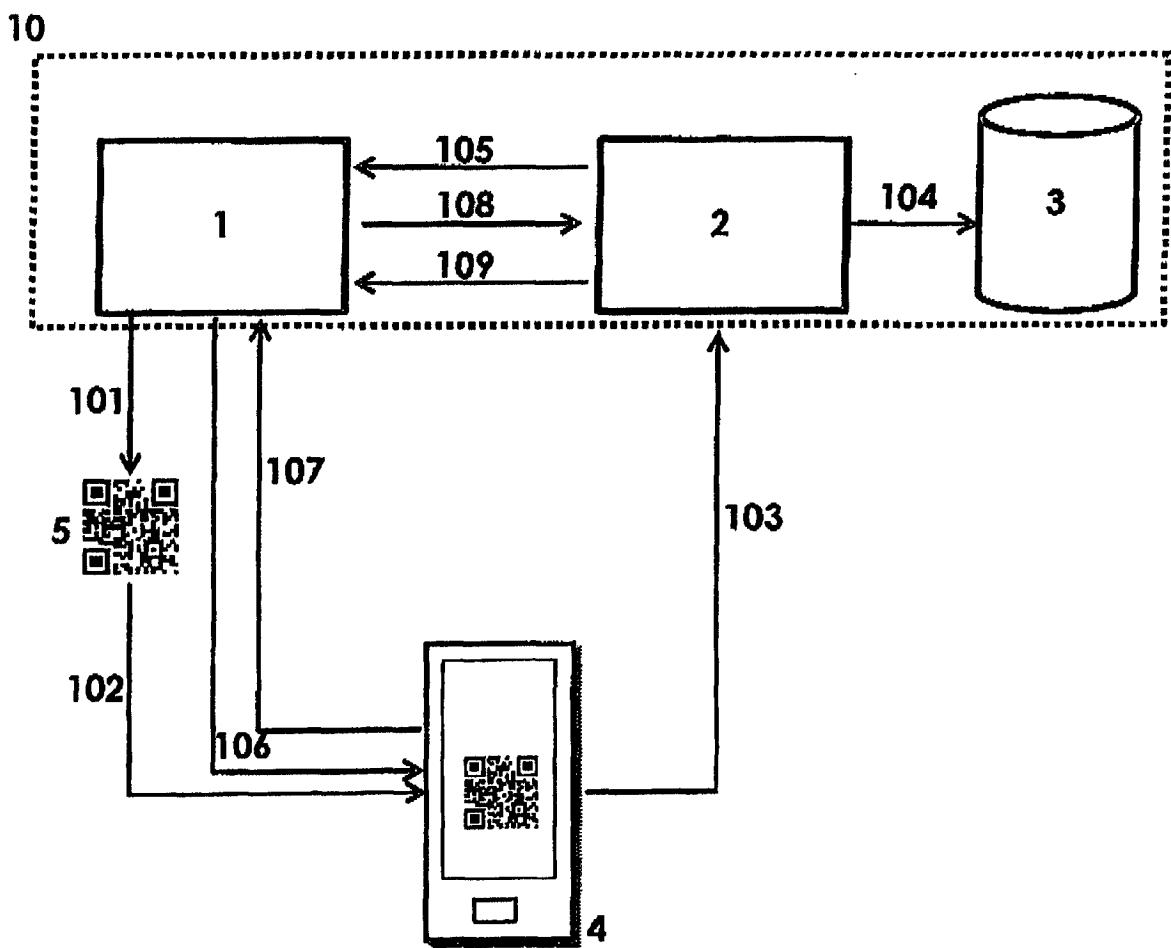


图 1