



(12) 发明专利

(10) 授权公告号 CN 109754048 B

(45) 授权公告日 2023. 10. 20

(21) 申请号 201811316779.2

(22) 申请日 2018.11.06

(65) 同一申请的已公布的文献号
申请公布号 CN 109754048 A

(43) 申请公布日 2019.05.14

(30) 优先权数据
17200196.8 2017.11.06 EP

(73) 专利权人 恩智浦有限公司
地址 荷兰埃因霍温高科技园区60邮编：
5656 AG

(72) 发明人 彼得·蒂林格 彼得·施马尔埃格
弗朗茨·阿姆特曼

(74) 专利代理机构 中科专利商标代理有限责任
公司 11021

专利代理师 倪斌

(51) Int.Cl.

G06K 19/07 (2006.01)

(56) 对比文件

CN 102999776 A, 2013.03.27

CN 106557716 A, 2017.04.05

US 2003174049 A1, 2003.09.18

US 2008018466 A1, 2008.01.24

US 2017103237 A1, 2017.04.13

WO 2011100939 A1, 2011.08.25

审查员 宋晓毓

权利要求书1页 说明书4页 附图2页

(54) 发明名称

电子标识装置

(57) 摘要

根据本公开的第一方面,提供一种电子标识装置,其包括超高频(UHF)通信单元,其中所述UHF通信单元被配置成受限制地启动。根据本公开的第二方面,构想一种操作电子标识装置的方法,所述电子标识装置包括超高频(UHF)通信单元,所述方法包括受限制地启动所述UHF通信单元。根据本公开的第三方面,提供一种非暂时性机器可读媒体,其包括在执行时实行所阐述种类的方法的指令。



1. 一种电子标识装置,包括为无线电通信单元的超高频UHF通信单元,其中所述UHF通信单元被配置成受限制地启动,

其中所述UHF通信单元被配置成由通过所述电子标识装置的近场通信NFC单元或高频HF通信单元接收的受保护启动命令启动,所述NFC单元或所述HF通信单元为基于电感耦合,

其中所述受保护启动命令借助于消息认证功能和/或加密功能而受到保护,并且所述受保护启动命令指定通过所述UHF通信单元可访问的存储器内容和/或存储器位置。

2. 根据权利要求1所述的电子标识装置,其中所述UHF通信单元被配置成使用定时器在预定义时间量内启动。

3. 根据权利要求2所述的电子标识装置,其中所述定时器被实施为带电荷电容器。

4. 根据在前的任一项权利要求所述的电子标识装置,其中所述UHF通信单元被配置成通过允许所述UHF通信单元和外部装置之间的单个通信会话来启动。

5. 根据权利要求4所述的电子标识装置,其中所述单个通信会话通过一次性密码启用。

6. 根据权利要求1到3中任一项所述的电子标识装置,其中所述UHF通信单元被配置成通过允许所述UHF通信单元和外部装置之间的多个通信会话来启动。

7. 根据权利要求6所述的电子标识装置,其中所述多个通信会话通过滚动密码启用。

8. 一种操作电子标识装置的方法,所述电子标识装置包括为无线电通信单元的超高频UHF通信单元,所述方法包括受限制地启动所述UHF通信单元,

其中所述UHF通信单元由通过所述电子标识装置的近场通信NFC单元或高频HF通信单元接收的受保护启动命令启动,所述NFC单元或所述HF通信单元为基于电感耦合,

其中所述受保护启动命令借助于消息认证功能和/或加密功能而受到保护,并且所述受保护启动命令指定通过所述UHF通信单元可访问的存储器内容和/或存储器位置。

9. 一种包括指令的非暂时性机器可读媒体,所述指令在执行时实行权利要求8所述的方法。

电子标识装置

技术领域

[0001] 本公开涉及一种电子标识装置。此外，本公开涉及一种操作电子标识装置的方法，并涉及一种对应的包括可执行指令的非暂时性机器可读媒体。

背景技术

[0002] 电子标识装置的例子是电子护照和电子身份证。电子标识装置通常包括高安全性非接触通信接口，例如在13.56MHz的频率下运行的近场通信(NFC)或高频(HF)通信接口，所述通信接口耦合到所述装置内的安全处理单元。此非接触通信接口能够实现相对较短距离内的通信。然而，在一些应用中，电子标识装置将得益于增加的通信距离。

发明内容

[0003] 根据本公开的第一方面，提供一种电子标识装置，包括超高频(UHF)通信单元，其中所述UHF通信单元被配置成受限制地启动。

[0004] 在实施例中，所述UHF通信单元被配置成由通过所述电子标识装置的近场通信(NFC)单元或高频(HF)通信单元接收的受保护启动命令启动。

[0005] 在实施例中，UHF通信单元被配置成使用定时器在预定义时间量内启动。

[0006] 在实施例中，所述定时器被实施为带电荷电容器。

[0007] 在实施例中，UHF通信单元被配置成通过允许所述UHF通信单元和外部装置之间的单个通信会话来启动。

[0008] 在实施例中，单个通信会话通过一次性密码启用。

[0009] 在实施例中，UHF通信单元被配置成通过允许所述UHF通信单元和外部装置之间的多个通信会话来启动。

[0010] 在实施例中，多个通信会话通过滚动密码启用。

[0011] 在实施例中，电子标识装置是电子身份证。

[0012] 在实施例中，电子标识装置是电子护照。

[0013] 根据本公开的第二方面，构想一种操作电子标识装置的方法，所述电子标识装置包括超高频(UHF)通信单元，所述方法包括受限制地启动所述UHF通信单元。

[0014] 在实施例中，所述UHF通信单元由通过所述电子标识装置的近场通信(NFC)单元或高频(HF)通信单元接收的受保护启动命令启动。

[0015] 在实施例中，UHF通信单元使用定时器在预定义时间量内启动。

[0016] 在实施例中，所述定时器被实施为带电荷电容器。

[0017] 根据本公开的第三方面，提供一种非暂时性机器可读媒体，其包括在执行时实行所阐述种类的方法的指令。

附图说明

[0018] 将参考附图更详细地描述实施例，在附图中：

- [0019] 图1示出电子标识装置的说明性实施例；
[0020] 图2示出操作电子标识装置的方法的说明性实施例；
[0021] 图3示出电子标识装置的另一说明性实施例。

具体实施方式

[0022] 电子标识装置通常包括高安全性非接触通信接口，例如在13.56MHz的频率下运行的近场通信(NFC)或高频(HF)通信接口。此非接触通信接口能够实现相对较短距离内的通信。然而，在一些应用中，电子标识装置将得益于增加的通信距离。例如，在电子护照或电子身份证的情况下，它将适用于在特定安全区域内确定护照或身份证在所述区域的入口处已经检查过，从而避免二次检查。NFC或HF通信接口在较远的距离无法实现此类确定。NFC或HF通信接口通常基于通信装置的天线线圈之间的电感耦合。

[0023] 因此，根据本公开，提供一种电子标识装置，其包括超高频(UHF)通信单元。UHF通信单元被配置成受限制地启动。超高频通信是指通信接口在大约300兆赫兹(MHz)和3吉兆赫(GHz)之间的范围内的频率下运行。这些接口能够实现较远距离的通信。UHF通信接口通常基于电磁波传输。

[0024] 应注意，例如电子护照的电子标识文件通常已经包括UHF通信单元，专门在制作所述文件期间用于后勤(logistic)目的。此类UHF通信单元通常是粘贴在文件中的物理分离的标签。在制作好所述文件之后，UHF通信单元被永久性地停用，以免在出厂后可能无意中通过UHF通信单元访问所述文件。UHF通信单元通常借助于标准化“终止(kill)”命令而被永久性地停用。相比之下，根据本公开，UHF通信单元被配置成受限制地启动，使得在电子标识文件出厂之后可以实现较大的通信距离。受限制启动缓解了通过启用电子标识文件的较大通信距离引入的安全性风险。

[0025] 在实施例中，UHF通信单元被配置成由通过电子标识装置的NFC单元或HF通信单元接收的受保护启动命令启动。启动命令可例如借助于消息认证功能和/或加密功能而受到保护。因此，UHF通信单元在电子标识出厂之前不会永久性地停用，而是可以(举例来说)借助于所述受保护启动命令重新启动。因为启动命令是受保护的，所以启动可以仅由经授权用户或装置执行或发起。并且，受保护启动命令通过NFC或HF接口传输，考虑到所述接口所支持的有限通信距离，这在本质上更加安全。UHF通信单元可集成到电子通信装置中，以便于通过所述NFC或HF接口接收启动命令。

[0026] 图1示出电子标识装置100的说明性实施例。电子标识装置100包括被配置成受限制地启动的UHF通信单元102。通过这种方式，可以实现较大的通信距离，同时还可缓解因为扩展的通信距离而引入的安全性风险。相比于NFC或HF通信单元，UHF通信单元的安全性较低。因此，可通过UHF通信单元获取的数据类型可限于(例如)标识符值或其它非关键数据。任选地，可通过UHF通信单元访问的存储器内容和/或存储器位置可在启动期间通过NFC或HF通信单元限定。举例来说，可访问的存储器内容和/或可访问的存储器位置可在受保护启动命令中指定。

[0027] 图2示出操作电子标识装置所阐述种类的方法200的说明性实施例。方法200包括在202处，初始化电子标识装置，并且在204处，受限制地启动UHF通信单元。因此，例如，电子标识装置可在出厂后进行初始化或个人化过程。在此初始化过程期间或在此初始化过程之

后,UHF通信单元可受限制地启动。

[0028] 在实际且高效的实施方案中,UHF通信单元被配置成使用定时器在预定义时间量内启动。因此,限制在于以下事实:启动是暂时的。换句话说,扩展的通信距离将仅在有限的时间量内可用。此外,在实际且高效的实施方案中,所述定时器被实施为带电荷电容器。带电荷电容器是定时器的高效实施方案,它不需要数字处理(例如)。此外,带电荷电容器不需要向装置供电。带电荷电容器随着时间推移失去电荷,并且如果电力再次接通——通过进入UHF场,那么装置可确定其余电荷是否高于预定义阈值。如果是,那么装置可得出结论:预定义时间量尚未结束。

[0029] 在实施例中,UHF通信单元被配置成通过允许所述UHF通信单元和外部装置之间的单个通信会话来启动。因此,在此实施例中,限制在于以下事实:仅允许单个通信会话。通过这种方式,安全性等级可保持相对较高。在实际且高效的实施方案中,单个通信会话通过一次性密码启用。此外,在实施例中,UHF通信单元被配置成通过允许所述UHF通信单元和外部装置之间的多个通信会话来启动。通过这种方式,可在安全性和用户便利性之间实现更好的权衡。在实际且高效的实施方案中,多个通信会话通过滚动密码启用。

[0030] 图3示出电子标识装置300的另一说明性实施例。电子标识装置300包括所阐述种类的UHF通信单元302。UHF通信单元302包括UHF模拟单元304、可操作地耦合到UHF模拟单元304的UHF数字核心306,以及可操作地耦合到UHF模拟单元304和UHF数字核心306的UHF密码单元308。根据本公开,UHF通信单元302受限制地启动。举例来说,UHF通信单元302可使用实施为带电荷电容器的定时器在预定义时间量内启动。带电荷电容器(未示出)可形成UHF模拟单元304的一部分。可替换地或另外地,UHF通信单元302可通过允许与外部装置(未示出)的单个通信会话或多个通信会话来启动。为此目的,UHF数字核心306可在分别验证接收到的一次性密码和滚动密码之后允许所述通信会话。用于对传送的数据进行加密和解密的密码支持可由高级加密标准(AES)密码单元318提供,UHF数字核心306耦合到所述密码单元318。应注意,所述密码支持可同样由图3中所示的三重数据加密标准(3DES)密码单元320提供。所述密码单元318、320通常在电子标识装置中是已经可用的,因为它们能够实现或支持通过近场通信(NFC)或高频(HF)通信接口的安全通信。任选地,UHF通信单元302可包括用于提供所述密码支持的上述UHF密码单元308。如图3所示,电子标识装置300的其它组件是HF模拟单元310、安全中央处理单元(CPU)312、ISO14443单元314、真随机数(TRN)生成器316、存储器管理单元(MMU)322、只读存储器(ROM)324、随机存取存储器(RAM)326,以及电可擦除可编程只读存储器(EEPROM)328,它们的功能总体上是技术人员已知的。具体地说,ISO14443单元314被配置成执行ISO/IEC 14443相关命令。ISO/IEC 14443是用于非接触智能卡在13.56MHz下运行的国际标准。UHF模拟单元304和HF模拟单元310可耦合到天线(未示出),所述天线能够实现与上述外部装置之间的通信。在实际实施方案中,模拟单元304、310耦合到分开的天线。此外,电子标识装置300包括HF/UHF单元330。HF/UHF单元330可为其中可存储非关键数据的共享存储器。HF/UHF单元330可(例如)为一次性可编程(OTP)非易失性存储器、多次可编程(MTP)非易失性存储器、电可擦除可编程只读存储器(EEPROM),或通过HF接口编写或增加的永久计数器。

[0031] 应注意,已经参考不同的主题描述了以上实施例。具体来说,一些实施例可能已参考方法类的权利要求来描述,而其它实施例可能已参考设备类的权利要求来描述。然而,本

领域的技术人员将从上述内容了解到,除非另有说明,否则除属于一种类型主题的特征的任一组合外,与不同主题相关的特征的任一组合,特别是方法类权利要求的特征和设备类权利要求的特征的组合,也被视为与此文档一起公开。

[0032] 另外,应注意图式为示意性的。在不同图式中,用相同的附图标记表示类似或相同元件。此外,应注意,为了提供说明性实施例的简洁描述,可能并未描述属于技术人员的习惯做法的实施细节。应了解,在任何此类实施方案的发展中,如在任何工程或设计项目中,必须制定大量实施方案特定的决策以便实现研发者的特定目标,例如遵守系统相关的和业务相关的约束条件,这在不同的实施方案中可能是不同的。另外,应了解,此类开发工作可能是复杂且耗时的,但仍然是本领域的技术人员进行设计、制造和生产的例行任务。

[0033] 最后,应注意,技术人员将能够在不脱离所附权利要求书的范围的情况下设计许多替代性实施例。在权利要求书中,置于圆括号之间的任何附图标记不应解释为限制权利要求。字词“包括”不排除在权利要求中列出的那些元件或步骤之外的元件或步骤的存在。元件之前的词“一(a/an)”并不排除多个此类元件的存在。权利要求书中叙述的措施可以借助于包括若干独特元件的硬件和/或借助于经适当编程的处理器来实施。在列出若干构件的装置权利要求中,可以通过硬件中的同一个物件实施这些构件中的若干个。在彼此不同的附属权利要求项中叙述某些措施这一单纯事实并不指示不能使用这些措施的组合来获得优势。

[0034] 附图标记列表

[0035] 100 电子标识装置

[0036] 102 UHF通信单元

[0037] 200 操作电子标识装置的方法

[0038] 202 初始化电子标识装置

[0039] 204 受限制地启动UHF通信单元

[0040] 300 电子标识装置

[0041] 302 UHF通信单元

[0042] 304 UHF模拟单元

[0043] 306 UHF数字核心

[0044] 308 UHF密码单元

[0045] 310 HF模拟单元

[0046] 312 安全中央处理单元

[0047] 314 ISO14443单元

[0048] 316 真随机数生成器

[0049] 318 AES密码单元

[0050] 320 3DES密码单元

[0051] 322 存储器管理单元

[0052] 324 只读存储器

[0053] 326 随机存取存储器

[0054] 328 电可擦除可编程只读存储器

[0055] 330 HF/UHF单元



图1

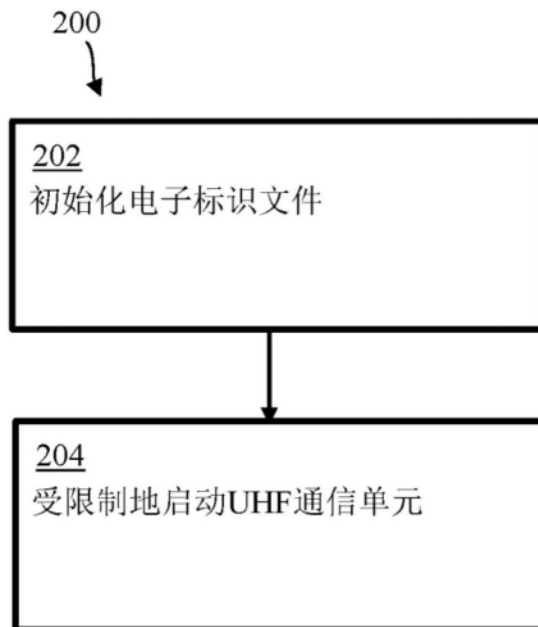


图2

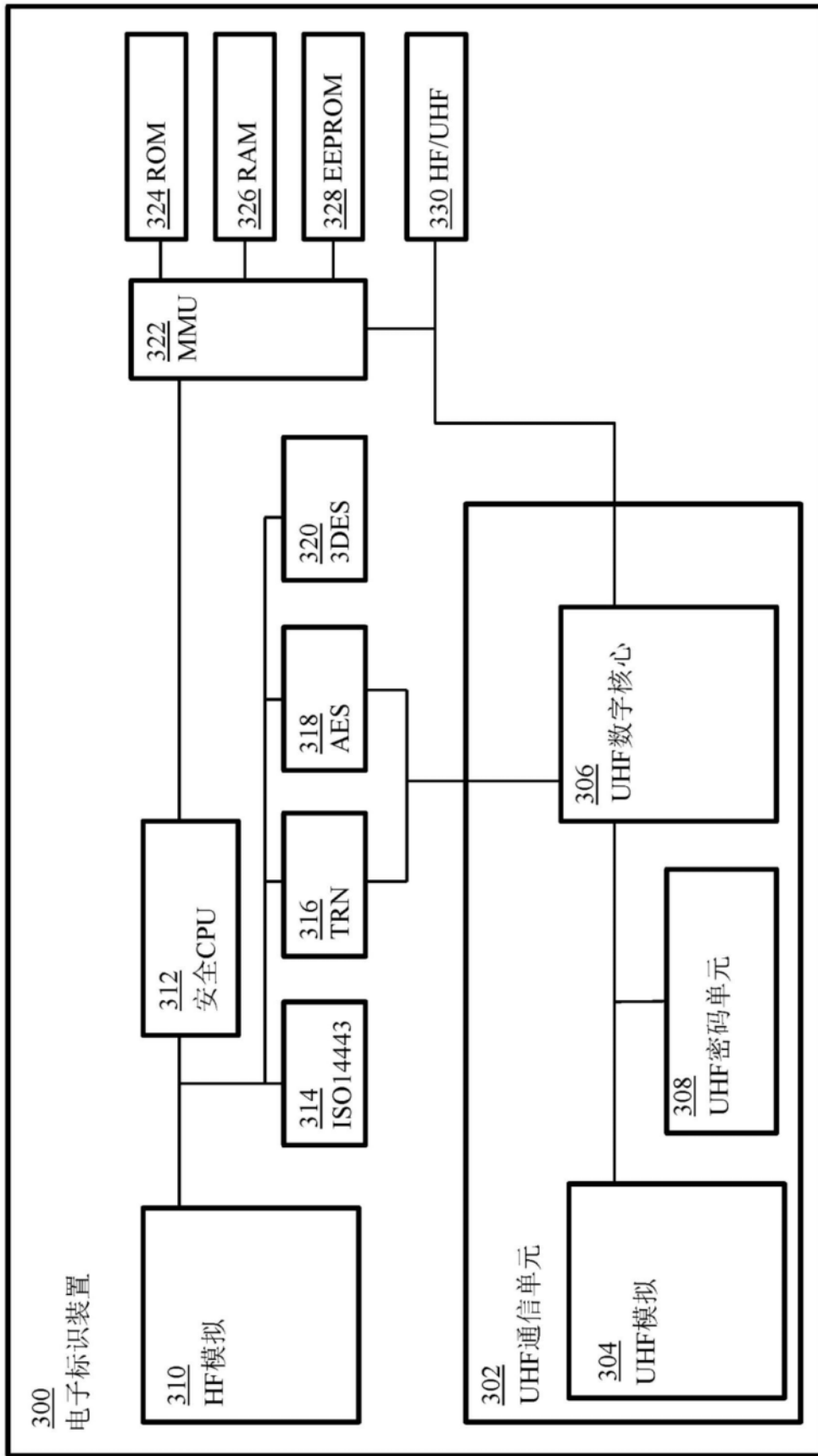


图3