国 际 电 信 联 盟

ITU-T X.1275

(12/2010)

国际电信联盟
电信标准化部门

X系列：数据网、开放系统通信和安全性

网络空间安全 – 身份管理

在应用RFID技术中保护个人可识别信息的指导原则

ITU-T X.1275建议书

国际电信联盟

ITU-T X 系列建议书

数据网、开放系统通信和安全性

公用数据网	X.1–X.199
开放系统互连	X.200–X.299
网间互通	X.300–X.399
报文处理系统	X.400–X.499
号码簿	X.500–X.599
OSI组网和系统概貌	X.600–X.699
OSI管理	X.700–X.799
安全	X.800–X.849
OSI应用	X.850–X.899
开放分布式处理	X.900–X.999
信息和网络安全	
一般安全问题	X.1000–X.1029
网络安全	X.1030–X.1049
安全管理	X.1050–X.1069
生物测定安全	X.1080–X.1099
安全应用和服务	
组播安全	X.1100–X.1109
家庭网络安全	X.1110–X.1119
移动安全	X.1120–X.1139
网页安全	X.1140–X.1149
安全协议	X.1150–X.1159
对等网络安全	X.1160–X.1169
网络身份安全	X.1170–X.1179
IPTV安全	X.1180–X.1199
网络空间安全	
计算网络安全	X.1200–X.1229
反垃圾信息	X.1230–X.1249
身份管理	**X.1250–X.1279**
安全应用和服务	
应急通信	X.1300–X.1309
泛在传感器网络安全	X.1310–X.1339
网络安全信息交换	
脆弱性/状态信息交换	X.1520–X.1539
事件/事故/探索法信息交换	X.1540–X.1549
政策的交换	X.1550–X.1559
探索法和信息请求	X.1560–X.1569
标识和发现	X.1570–X.1579
确保交换	X.1580–X.1589

欲了解更详细信息，请查阅 ITU-T建议书目录。

ITU-T X.1275建议书

在应用RFID技术中保护个人可识别信息的指导原则

摘要

建议书ITU-T X.1275认识到，虽然射频身份识别（RFID）技术促进了有关个人穿着或携带的商品的信息获取和传播（以用于有益目的），但也使这种信息面临被滥用的风险。这种滥用可表现为追踪当事人的位置或以另一种不正当的方式侵犯其个人隐私。为此，本建议书提供有关RFID程序的指导原则，从而在享受RFID优势的同时尽力保护个人可识别信息。

沿革

版本	建议书	批准日期	研究组	
1.0	ITU-T X.1275	2010-12-17	17	

关键词

保护个人可识别信息，RFID应用。

前言

国际电信联盟（ITU）是从事电信领域工作的联合国专门机构。ITU-T（国际电信联盟电信标准化部门）是国际电信联盟的常设机构，负责研究技术、操作和资费问题，并且为在世界范围内实现电信标准化，发表有关上述研究项目的建议书。

每四年一届的世界电信标准化全会（WTSA）确定ITU-T各研究组的研究课题，再由各研究组制定有关这些课题的建议书。

WTSA第1号决议规定了批准建议书须遵循的程序。

属ITU-T研究范围的某些信息技术领域的必要标准，是与国际标准化组织（ISO）和国际电工技术委员会（IEC）合作制定的。

注

本建议书为简明扼要起见而使用的“主管部门”一词，既指电信主管部门，又指经认可的运营机构。

遵守本建议书的规定是以自愿为基础的，但建议书可能包含某些强制性条款（以确保例如互操作性或适用性等），只有满足所有强制性条款的规定，才能达到遵守建议书的目的。“应该”或“必须”等其它一些强制性用语及其否定形式被用于表达特定要求。使用此类用语不表示要求任何一方遵守本建议书。

知识产权

国际电联提请注意：本建议书的应用或实施可能涉及使用已申报的知识产权。国际电联对无论是其成员还是建议书制定程序之外的其它机构提出的有关已申报的知识产权的证据、有效性或适用性不表示意见。

至本建议书批准之日止，国际电联尚未收到实施本建议书可能需要的受专利保护的知识产权的通知。但需要提醒实施者注意的是，这可能并非最新信息，因此特大力提倡他们通过下列网址查询电信标准化局（TSB）的专利数据库：http://www.itu.int/ITU-T/ipr/。

目录

ITU-T X.1275建议书

在应用RFID技术中保护个人可识别信息的指导原则

1 范围

本建议书为射频身份识别（RFID）用户和厂商（包括RFID服务提供商和产品制造商）提供有关保护个人可识别信息的指南，以维护RFID技术环境中的个人隐私。

这些指导原则适用于利用RFID系统侵犯个人隐私的情况，如，在RFID标签中记录个人可识别信息，随后对其进行收集，或将通过RFID收集的物体（object）信息与个人可识别信息相联系。然而，对于收集和使用物体信息不会带来泄漏个人可识别信息和侵犯隐私的情况，这些指导原则并不适用。

这些指导原则旨在保护个人隐私可能受到RFID系统影响的个人可识别信息，并促进发展安全的RFID使用环境。制定这些指导原则的意图在于为RFID服务提供商提供基本规则，并就RFID中的隐私问题为RFID服务提供商、产品制造商和用户提供指南，同时这些指导原则须服从本地和国家法律。

2 参考文献

下列ITU-T建议书和其它参考文献的条款，在本建议书中的引用而构成本建议书的条款。在出版时，所指出的版本是有效的。所有的建议书和其它参考文献均会得到修订，本建议书的使用者应查证是否有可能使用下列建议书或其它参考文献的最新版本。当前有效的ITU-T建议书清单定期出版。本建议书引用的文件自成一体时不具备建议书的地位。

[ISO/IEC 18000] ISO/IEC 18000-6 (2004), *Information technology – Radio frequency identification for item management – Part 6: Parameters for air interface communications at 860 MHz to 960 MHz.*

[ISO/IEC 19762-3] ISO/IEC 19762-3 (2005), *Information technology – Automatic identification and data capture (AIDC) techniques – Harmonized vocabulary – Part3: Radio frequency identification (RFID).*

3 定义

3.1 其它资料规定的术语

本建议书采用了下列其它资料规定的术语：

3.1.1 personally identifiable information (PII) [ITU-T X.1171] **个人可识别信息**：与活着的人相关的信息，可用以识别该个人（包括能够与其它信息合并识别一个人的信息，即使该信息并非明确识别该人）。

3.1.2 radio frequency identification (RFID) system [ISO/IEC 19762-3] **射频身份识别（RFID）系统**：由一个或多个识读器/询问器及一个或多个转发器构成的自动识别系统和数据捕获系统，其实现数据传送的手段是得到适当调制的感应或辐射电磁载波。

3.1.3 radio frequency identification (RFID) tag [ISO/IEC 19762-3] **射频身份识别（RFID）标签**：任一转发器及附着于物体的信息存储机制。

3.2 本建议书确定的术语

本建议书定义了下列术语：

3.2.1 consent 同意：为数据收集器提供入或出协议，以收集、转移、使用、存储、归档或处理掉具体PII、有意义的个人、有限协议。

3.2.2 data controller 数据控制方：将记录于RFID标签中的物体信息与PII进行联系，或在RFID标签中记录PII，或收集在RFID标签中得到记录的PII的实体。

3.2.3 data subject 数据主体：可通过一项或多项涉及其身体、心理、意识、经济、文化或社会属性的数据对其进行识别的实体。

3.2.4 opt-in 选定加入：个人明确同意PII收集方为某一具体目标而收集、传送、使用、存储、归档或处理掉具体PII。

3.2.5 opt-out 选定退出：个人通过要求进行的数据的特定收集、传送、使用、存储、归档或处理不会出现的选择。

3.2.6 personal data 个人数据：见个人可识别信息。它是个人可识别信息的同义词。

3.2.7 radio frequency identification (RFID) manufacturer射频身份识别（RFID）制造商：制造和销售RFID芯片/标签或制造（包括处理或包装）和销售带有内置附着RFID标签的物体的实体。

3.2.8 radio frequency identification (RFID) service provider射频身份识别（RFID）服务提供商：提供基于带有内置或附着RFID标签的物体的服务的任何实体。

3.2.9 user 用户：购买带有内置或附着RFID标签物体的个人或使用基于带有内置或附着RFID标签物体的服务的个人

4 缩写词和首字母缩略语

本建议书采用了下列缩写词和首字母缩略语：

AES 先进加密标准

NFC 近场通信

PDA 个人数字助手

PIA 隐私影响评估

PII 个人可识别信息

RFID 射频识别

5 惯例

无。

6 隐私原则

本建议书所述指导原则以包含在以下文件中的隐私原则为基础：[b-Council of Europe]、[b-EC1]、[b-EC2]、[b-OECD]、[b-UNHCR]。这些原则特别包括：

– 收集限制：对个人信息的收集应有限度，应通过合法和公平手段并在数据主体知情和同意情况下获得此类数据。

– 数据质量：个人数据应与其用途相符，且应尽可能在实现目的方面做到准确、完整，并保持得到更新。

– 确定目的：应在收集数据之前确定收集个人数据的目的，且数据的随后使用应限于满足这些目的，或满足并非与这些目的相吻合但在每一次目的发生变化时均得到具体明确的其它目的。

– 使用限制：个人数据不应被披露、提供或用于所具体明确目的以外的其它目的。

– 安全保障：应通过合理的安全保障机制保护个人数据不受到丢失、被非法获取、销毁、使用、修改或披露等风险的影响。

– 开放性：应制定关于个人数据制定、做法和政策开放性的总体政策。应随时提供可以确立个人数据存在和性质及其主要使用目的和数据控制方的身份及常驻地址的手段。

– 个人参与：个人应有权：

a) 从数据控制方或其它处得到有关数据控制方是否拥有有关他/她个人数据的确认；

b) 在合理时间内得到有关涉及到他个人的数据方面的情况说明，且如果在实行收费情况下，收费不应过渡；方法合理；形式应是其能即刻读懂的形式；

c) 如果其按照a) 和b) 分段提出的请求被拒绝则应得到相应理由，且应能对这种拒绝行为提出质疑；

d) 对涉及到他个人的数据提出质疑，且如果该质疑得到确认，则可以删除、修改、补充完整或修正所述数据。

– 问责：应就遵守实现上述原则的相关机制对数据收集方进行问责。

7 RFID中PII面临的威胁和侵犯

RFID中PII面临的威胁和侵犯主要由RFID技术的非接触特性、无线通信技术的脆弱性和第三方通过RFID识读器收集数据的可能性造成。附录II详细阐述RFID技术的特性。

此外，RFID技术的引入导致了PII侵犯现象的日益加剧，因为数据收集方通过RFID标签获得的信息可在整个网络中得到使用，而非按照国家或区域性法律、规则和政策得到使用，同时，还可以通过修改该信息来得出PII。下一节将阐述RFID技术为PII带来的主要威胁和侵犯。

然而值得注意的是，由于现有RFID标签使用诸如电力、处理时间、存储空间等资源，因此在这类标签中纳入一些安全机制可能十分困难。附录I和II说明RFID技术的限制及RFID系统的技术保护措施。

7.1 数据收集的隐蔽性

由于RFID技术存在一些特定特性，因此数据收集可在数据主体不知情的情况下进行。RFID标签中的数据可在没有任何直接视距的情况下得到识读，因为无线电波可以穿透诸如背包或衣服等障碍物，因此，任何拥有识读器的人均可识读RFID标签中的数据。此外，RFID标签及识读器的尺寸可以做到很小，因此可以不露痕迹地对其进行操作。这一特点是造成RFID技术中PII被侵犯的原因之一。

7.2 个人资料

获得由数据主体拥有或携带的物体中的RFID标签信息可暴露有关该个人的隐私或喜好。特别值得一提的是，通过数据主体携带的一系列RFID标签得出的个人资料和推理则可暴露敏感信息。此外，RFID应用（如电子护照和使用RFID技术的医疗应用）可暴露国籍、生物特征信息或病例等更为敏感的信息，并可被直接用于制定有关数据主体的个人资料和推理等。

7.3 跟踪

可对携带RFID标签的数据主体进行跟踪，因为已为RFID标签分配了独一无二的标识符。

通过收集或处理有关位置和时间的数据即可进行跟踪，并可以随后方式（数据已存储在数据库中）或实时方式进行跟踪。

8 RFID应用

RFID技术被广泛用于种类繁多的应用，包括医疗、交通和物流、电子政务和支持零售及供应链的信息服务。表1所列为使用RFID技术的典型应用可能对PII造成的威胁。

表 1 – 典型RFID应用及可能对PII形成的威胁

领域	典型应用	RFID标签中的信息	可能对隐私造成的威胁
供应链	库存管理	产品	跟踪、形成个人资料 执行库存
	零售（如超市）	产品	跟踪、形成个人资料 （购买货物之后）
交通和物流	公共交通票证	用户身份、收费等	跟踪、形成个人资料
	公路收费	用户身份、收费等	跟踪、形成个人资料
	车辆跟踪	产品	跟踪、形成个人资料
	车队/集装箱管理	产品	跟踪、形成个人资料 处理集装箱

表 1 – 典型RFID应用及可能对PII形成的威胁

领域	典型应用	RFID标签中的信息	可能对隐私造成的威胁
医疗	跟踪病人	病人身份、医疗历史记录等	跟踪、形成个人资料、隐蔽性
	防止用药错误	病人身份、医疗历史记录、处方等	跟踪、形成个人资料
	对血液或药品进行跟踪，防止假冒	产品	×
电子政务	电子护照	个人身份、国籍、生物特征	跟踪、形成个人资料、伪造PII
信息服务	智能招贴画	产品	×

如表1所示，并非所有RFID应用均会造成对PII的侵犯（也并非所有这些应用均会带来潜在问题）。例如，如果RFID应用不包含用户，在某些供应链应用中，可能不会出现对PII的侵犯情况。

然而，如工人是在其它供应链应用中处理集装箱，可以使用RFID标签控制这些工人的活动。

以下各分节通过具体服务情形说明可能造成对PII侵犯的某些应用示例。

RFID识读器及其它（如移动）应用合并一起时会带来多种通信关系，这种情况会加强有关方面做出跟踪和形成个人资料的能力。

8.1 供应链管理

长期以来，RFID技术已被广泛用于供应链管理工作。使用RFID进行供应链管理的主要业务应用包括库存/资产管理，零售应用等。零售是最具代表性的RFID应用服务。图1以零售应用对RFID使用的示例说明RFID标签的分布情况。

RFID零售应用由制造RFID标签、将物体信息写入RFID标签并将标签附着于物体的制造商实现。在该示例中，所述零售商为将带有RFID标签的物体销售给用户的RFID服务提供商。在供应链管理中，通常使用RFID系统的无源标签，并通过灭活口令（kill password）等保护数据主体的PII。在用于个人物品等应用的某些情况下，供应链管理往往要求使用具有长通信距离的无源标签（即使个人物品也是如此）。

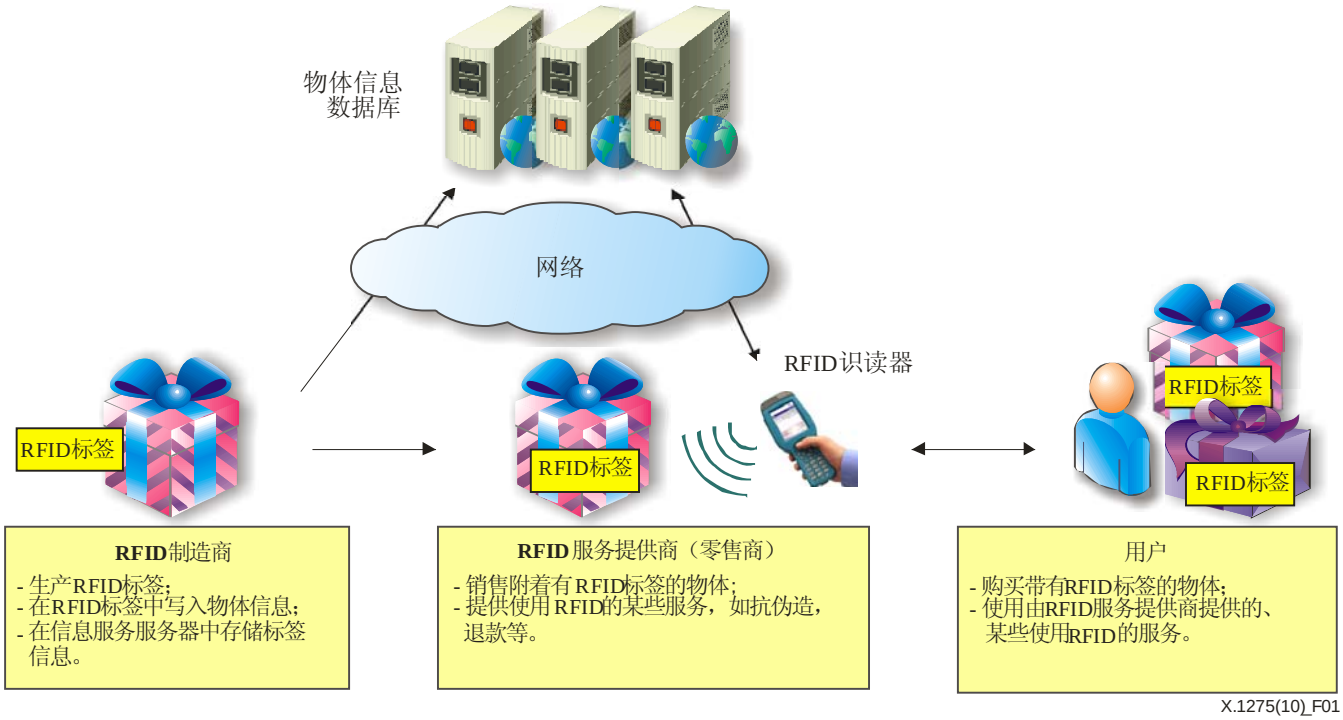


图 1 – 零售应用使用RFID的示例

在用户购买附着有RFID标签的一个物品之后往往会出现零售应用中对PII的侵犯情况，因为在此过程中，用户仅在销售时刻予以参与。当用户购买带有RFID标签的物品时，零售商可通过将存储于RFID标签中的物品信息与用户支付信息或积分卡相联系，并通过持续不断观察和分析用户的购买规律来确定该用户的喜好。在这种情况下，RFID服务提供商变成数据控制方，用户变为数据主体。此外，拥有识读器的任何个人均可识读RFID标签，除非取消或销毁该标签。

8.2 交通和物流

RFID系统非常适合于某些交通和物流应用。如果很好地对RFID识读器进行分布，则带有标签的车辆可在小范围（如仓库或工厂）内得到跟踪。在交通和物流行业，带来隐私问题的应用是公共交通票证和公路费收费系统（如[b-E-Zpass]所述系统）。

交通和物流领域存在若干RFID应用，特别值得指出的是，许多公共交通票证和公路收费系统均已采用RFID技术。图2以交通应用示例说明如何采用RFID标签来识别和跟踪公路收费系统中的车辆。

RFID制造商在公路收费应用中仅需制造RFID标签并将其销售给RFID服务提供商。提供和管理公路收费服务的RFID服务提供商可在某些具体下将用户付费信息写入RFID标签。RFID标签中存储的用户付费信息就是可方便识别该用户的PII。

如果用户付费信息与公路收费系统记录的用户移动跟踪信息相关联，则这种信息会严重威胁到用户的隐私。在这种情况下，RFID服务提供商 – 公路收费系统 – 就成为数据控制方，而用户则成为数据主体。

通常交通和物流领域使用的RFID系统采用无源标签。在交通领域内，一般使用轻型加密方案（基于对称加密方案）进行标签和识读器之间的认证，为进一步数据传输提供安全保证。

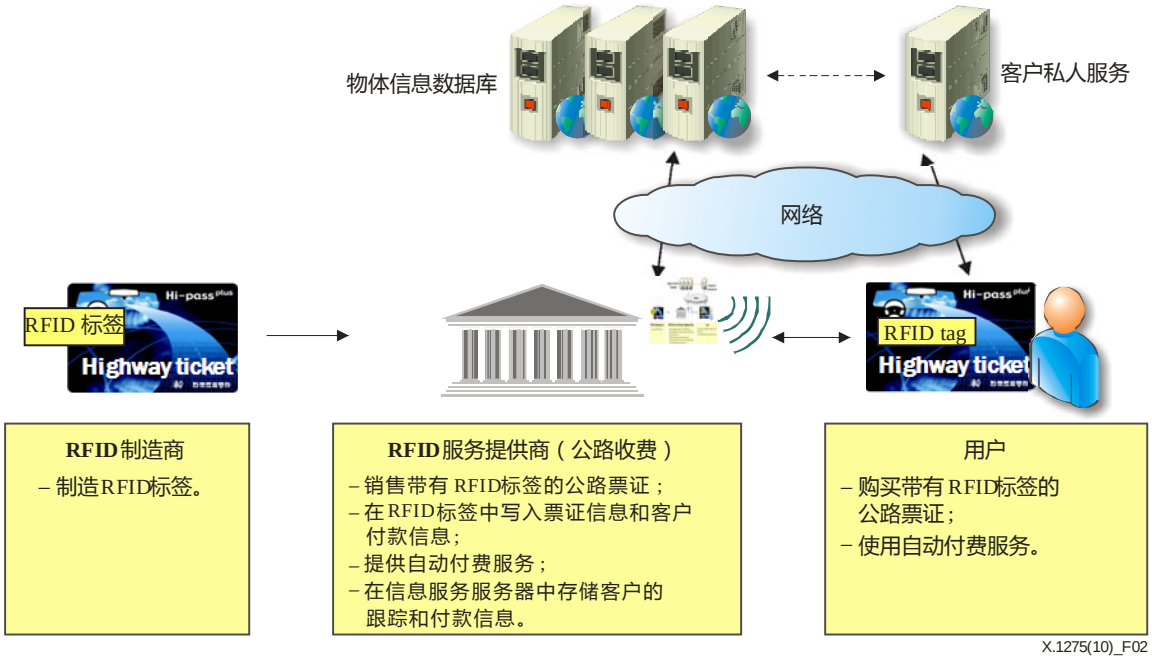


图2 – RFID用于交通和物流领域的示例

对交通票证而言，常常使用以在13.56 MHz通信且通信距离较短的RFID芯片制造的无接触智能卡。对于阅读距离较短的标签，使用传统的加密机制（甚至非对称机制）至少在技术上是可行的，可以部分降低泄露数据主体PII的风险。然而，值得注意的是，目前使用的协议只能防止复制标签（从而防止篡取用户信息）。标鉴身份在标签和识读器交易之初便暴露于文本的字里行间，因此可被任何人识读，由此带来侵犯PII的风险。在任何情况下，当用户与系统互动时，数据库中收集的数据应尽快匿名，以便降低对用户隐私造成的威胁。

8.3 卫生和医疗应用

RFID可用于若干卫生医疗应用之中，然而，由于医疗卫生数据为敏感的涉及个人隐私的数据，因此RFID在医疗卫生应用方面的使用会带来侵犯PII的风险。RFID在医疗卫生领域的应用包括为安全起见跟踪病人、防止造假药品的措施、遵循病人处方并对血液进行跟踪。医药行业已在通过RFID系统方便药品跟踪，以防止药品伪造及在运输过程中的丢失。图3为RFID在医疗卫生应用方面的使用示例，具体说明如何使用RFID标签。

按照患者处方生产RFID的制造商仅需制造RFID标签并予以销售。RFID服务提供商，即医院的医生和护士是数据控制方，负责书写和管理病人的医疗信息。

在图3所示的应用中，医院的医生和护士可通过阅读病人携带的RFID标签中的信息了解患者的既往治疗史和处方情况，并随后以此为基础采取适当行动。相反，在药品跟踪应用中，医院或药店以外持有带标签的药品的人员的标签信息可轻而易举地被泄露，且可通过

RFID标签信息直接通过推理得出患者所患疾病名称，因此，数据主体个人信息被披露的风险可能高于图2所示应用的情况。有鉴于此，如果不能很好地管理和保护存储于RFID标签或后台数据库中的患者医疗信息，则会对数据主体的PII产生直接威胁。

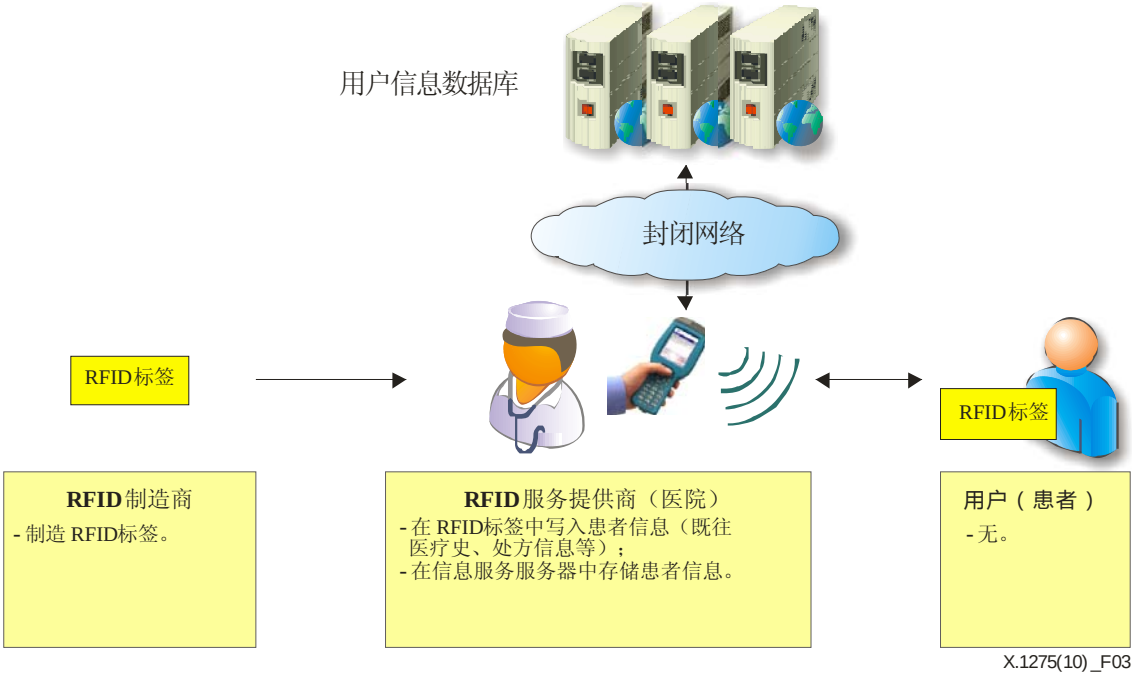


图 3 – RFID在卫生和医疗应用方面的使用示例

卫生医疗应用领域通常不使用RFID系统的长通信距离有源标签。但是，某些情况下可能人们更希望使用具有长通信距离的有源标签，如家庭医护工作中对病人病情的监测。

8.4 电子政务

电子护照是电子政务中最为典型的应用。嵌入电子护照中的RFID芯片往往包含数据主体的诸多PII，如护照号码、姓名、国籍、生物特征信息等，因此很可能带来很大的侵犯PII的风险。

重要的是，RFID标签能与适当的安全措施结合起来以降低电子护照数据的捕获或克隆风险，因为电子护照中的数据是最为重要和关键的PII。图4给出了RFID在电子护照系统中的使用示例，显示RFID芯片的使用方式。

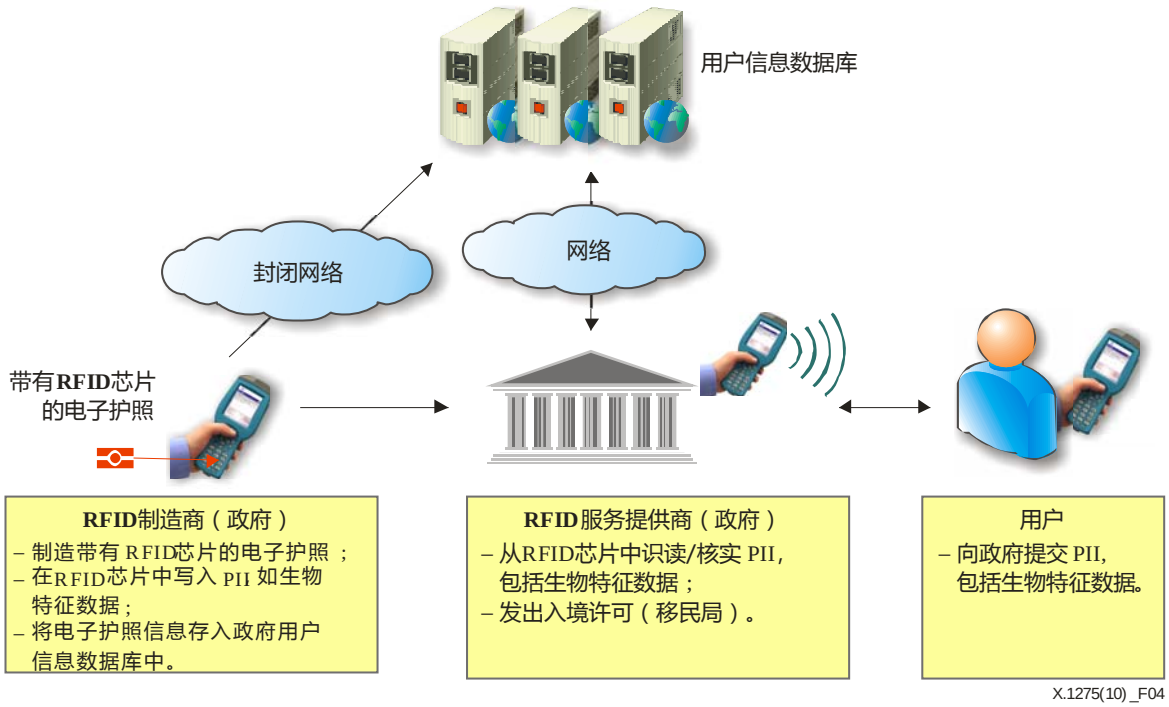


图4 – RFID在电子护照应用领域的使用示例

希望得到具有生物特征的电子护照的用户向政府相关部委提交包括生物特征数据在内的PII，后者可以是电子护照应用的RFID制造商。制造商制造带有RFID芯片的电子护照，并在芯片中写入包括生物特征数据的用户PII。RFID服务提供商（如移民局）从RFID芯片中识读PII，并对其进行核实。电子护照RFID芯片中存储的生物特征数据是最为敏感的PII之一，可用于认证或识别用户。这些数据如被披露或修改，则会严重威胁到用户隐私。在该应用中，RFID制造商和RFID服务提供商均可以是数据控制方，用户则为数据主体。通常该应用采用具有短通信距离的无源标签。电子护照须支持加密。

然而，[b-ICAO]等标准描述的安全协议有时为可选协议，或使用极不洽当，因此，电子护照应用领域仍然存在很大的侵犯个人隐私的风险。

8.5 信息服务

智能招贴画是信息服务应用领域的典型示例。在智能招贴画中，RFID识读器往往安装在移动装置中，RFID标签则置于固定地点。图5所示为RFID在智能招贴画应用领域中的使用示例，具体说明如何使用RFID标签和识读器。

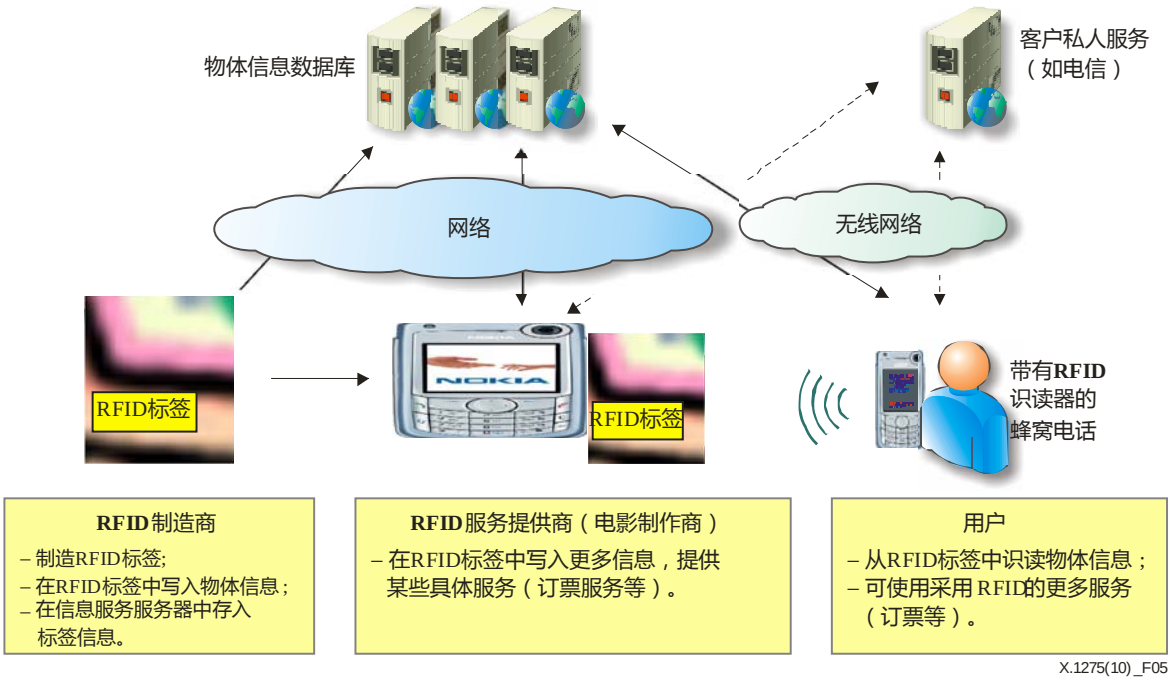


图5 – RFID在智能招贴画应用领域的使用流程

智能招贴画RFID制造商仅需制造RFID芯片并将其销售给RFID服务提供商。电影制做商或影剧院为RFID服务提供商，将有关电影的信息写入内置在智能招贴画中的RFID标签中。在信息服务其它示例中，我们可以例举公路指南服务，通过该服务向用户提供相关信息，使其轻松找到要去的方向。这种应用事实上不会带来个人隐私方面的风险，因为应用不使用任何个人或敏感信息。然而，值得注意的是，嵌入移动装置中的RFID识读器的移动和识读范围可能会对用户隐私造成威胁。

9 有关保护个人可识别信息的指导原则

由于涉及RFID的隐私和安全技术尚处于初级发展阶段（即使其正在发展），因此在RFID标签的使用和技术特性方面不存在“万全”良策，因为此类标签在不同应用中的使用大相径庭，将其用于整个RFID服务仍然为时过早。有鉴于此，本节所述指导原则重点关注保护数据主体PII的一般性管理措施而非技术措施。即便如此，也不能忽视技术措施：在构思基于RFID的应用时，应鼓励设计人员考虑采用最新的、可以提高隐私保护的技术解决方案。

9.1 政策和程序

RFID服务数据控制方应制定规范RFID系统的政策和程序，特别是关于洽当使用PII的政策和程序，并事先公布。此类政策和程序应明确有关方面在管理和使用PII方面的作用和职责。此外，数据控制方应为直接负责管理和使用PII的人员分配更多职责。

9.2 记录PII的限制

数据控制方应遵守收集限制原则。因此，控制方须只处理与系统设计目标相关的数据，PII的存储不得超过必要的时间。

尤其值得一提的是，RFID服务中的数据控制方通常不应在RFID标签中记录PII，除非法律明确规定或数据主体通过书面同意记录PII。如果数据控制方不得不将PII记录在RFID标签中，RFID标签中记录的所有PII必须加密。当数据控制方需要数据主体同意时，最好选定加入。数据控制方必须事先通知数据主体有关记录和使用PII的目的。

RFID服务中的数据控制方须就每一项记录的PII获得个人的具体同意，同时将记录和使用PII的目的通知数据主体。

9.3 信息、同意、获取权、核准、反对权

数据控制方须遵守个人参与原则。因此，RFID服务中的数据控制方要采取适当措施，在不为用户带来任何代价的情况下，就提供有关记录的PII的用户信息和对数据主体PII的同意、获取权、核准和反对权。这适用于已在IFID标签上获得编码的PII以及与存储在RFID标签中信息相关的PII。

9.3.1 信息

数据控制方应通知数据主体有关附着RFID标签和RFID识读器安装的提示、数据所披露的第三方的核准、封锁的取消，除非证明不可能做到或需要付出不必要的努力。

9.3.1.1 附着RFID标签的提示

对内置或附着的RFID标签而言，即使在用户购买或收到物体之后，RFID服务中的数据控制方仍须在购买物体之前事先向用户做出下列解释，或指明物体上的信息，或使用某种极易被注意到的手段：

– 已附着了RFID标签及其位置。

– RFID 标签的性质和功能。

– RFID 标签中所记录信息的类别。

– RFID 标签中记录的信息的目的或使用情况。

– 按照第9.9节提供数据保护官员的联系方式。

请注意，如数据主体在购买物体后并非自用，RFID服务或数据控制方应在用户购买了标签物体后立刻中止标签活动，除非用户决定保留工作中的标签。

9.3.1.2 表明已安装RFID识读器

安装能够识读带有内置或附着RFID标签（或记录在RFID标签中的PII并提供给数据主体）的物体上的信息的识读器的人均须表明已安装了识读器，以便数据主体极易注意到这一事实。通知应至少包括运营商的身份和个人可获得有关服务信息政策的联系人。

如RFID识读器为内置于个人PDA或移动电话的识读器，则识读器的识读范围必须得到限制，以避免通过RFID标签得到PII信息。

9.3.2 同意

数据控制方需要事先获得数据主体的同意。在零售和物流的情况中，如原则是默认取消，数据控制方可通过获得具体的书面协议、用户注册表、电子邮件等得到数据主体的同意。在其它情况下，如具有生物特征的电子护照应用中，不需要用户同意，因为收集PII并将其保存在标签中是一项法律义务。

9.3.3 获取权、核准和反对权

数据主体应能在没有合理期限限制和过分拖延或支出的情况下从数据控制方获得：

– 有关数据主体的数据是否得到处理以及起码的处理目的信息、有关数据披露的接受者或接受者类别信息的确认，

– 以无形数据形式向数据主体提供的有关正在处理的数据和任何有关数据来源的可用信息的通信，

– 有关数据主体的数据至少在自动决策情况下自动处理所涉及逻辑知识

此外，RFID服务中的数据主体需采取适当措施，向用户提供无需用户成本即可纠正、修改和销毁数据主体PII的方法。

这种方法适用于编码在RFID标签中的PII，以及与储存在RFID标签中的信息相关联的PII。

特别值得一提的是，如标签对于数据主体而言无用（如在零售行业，当用户购买了标签项目后），数据控制方需要按第9.5节所讨论的方式取消、除去或销毁标签，除非数据主体要求保留该标签的工作状态。

9.4 收集和联系PII的限制

RFID服务中的数据控制方应在收集记录在标签或存储在数据库中的PII时通过将标签中的物体信息相结合通知相关数据主体。如RFID服务提供商需要使用PII用于计划以外的目的或将此信息提供给第三方，他们需要事先获得数据主体以书面形式提供具体知情同意。

9.4.1 记录在RFID标签中的PII

RFID服务中的数据控制方需要以易注意到的方式向相关数据主体发出通知或提示，使他们可以收集记录在RFID标签中的PII并事先获得用户的具体和知情同意。

当数据控制方收集PII时，他们须对RFID识读器和标签采取认证措施，如在RFID标签和识读器之间以及识读器和后端数据库之间采用认证协议。在此，“认证措施”指为存储RFID标签标识符的后端数据库采用加密方案。PII用来识别和认证RFID识读器和数据控制方。

但从PII保护角度而言，应指出，现有标签和识读器之间的认证协议只有在标签存储的信息超过标签身份内容的情况下才有效。使用现有RFID传输协议，标签身份本身不受保护。

9.4.2 RFID标签中于PII相关的物体信息

如数据控制器希望将记录在RFID标签中的物体信息与PII相结合，一般情况下，应在提供标签以前以易注意到的方式事先通知数据主体，以便获得具体的知情同意。当数据控制方将RFID标签中的物体信息与PII相结合时，他们应对RFID识读器采取一些认证措施，如口令或在RFID识读器和标签之间的认证协议。

如在收集PII时，不用将其与物体信息相结合而是在晚些时候结合，数据控制方则应将此目的通知用户并按照法律要求获得进一步具体和知情的同意。

9.5 在实现目的后中止RFID标签活动

RFID服务提供商或数据控制方在用户购买或收到标签物体（销售点）时应取消、销毁或永久中止RFID标签活动，除非用户决定保留标签的工作状态，或法律法规要求保持标签的激活状态。尽管用户决定保留标签的工作状态，数据控制方须提供措施在晚些时候按照数据主体的要求取消、销毁或永久中止标签活动。用户应得到有关中止标签活动的后果通知。

中止标签活动被要求作为正常情况，但它并非适用于各项应用。举例而言，如用来了解医疗应用中患者的治疗记录和处方信息的标签被中止活动后，患者的连续治疗可能变得异常困难。在供应链管理中中止标签活动是强制性的，但在交通和物流的应用中，中止活动是用户的选择。在医疗和电子政务应用中，中止活动不适用于公共卫生或在法律是不允许的。RFID制造商或RFID服务中的数据控制方可使用一些技术手段中止RFID标签活动，如灭活口令，RFID灭杀器。如中止RFID标签活动影响用户的利益或公众利益，数据控制方可以向用户说明原因或提示物体中的标签或使用易注意到的方式。

9.6 有关服务提供商和数据控制方的信息

服务提供商和数据控制方应为各项应用拟定并公布言简意赅和方便易懂的信息政策。这些政策至少包括：

– 控制方的身份和地址，

– RFID系统的目的，

– 系统要处理哪些数据，特别是在处理个人数据时，是否监督标签位置，

– 隐私和数据保护影响评估摘要，

– 在应用中使用标签可能产生的隐私风险（如有的话）和个人可采取的缓解风险的措施。

9.7 保护PII的组织和技术措施

– 当RFID服务的数据提供方使用RFID系统记录或收集PII，或将RFID标签的物体信息与PII相联系时，他们应采取组织和技术安全措施保护RFID的PII，以防止相关PII的丢失、被窃、泄漏、被修改或损坏。保护PII的组织和运行措施包括：

  • 内部安全管理计划；

- 风险分析，隐私威胁分析和隐私影响评估；
- 就有关RFID服务的隐私问题开展教育等。

– 保护PII的技术措施包括：

- 访问控制和后台数据库审计；
- 采取接入控制，防止识读器获得存储在标签中的信息；
- 存储在标签和后台数据库中的PII的加密；
- 采用识读器和标签之间任何可行的协议保护PII的传送，如加密协议，或相关的技术；
- 使用实施随机标签标识符的标签减少跟踪风险；
- 对有效RFID识读器进行认证；
- 终止RFID标签活动，如灭活口令、RFID灭杀器等；
- 限制识读器和标签的能力，如有源干扰、RFID传感器识别、消波标签（clipped tag）、封锁标签（blocker tag）等[b-Juels]；
- 降低因隐私影响分析（PIA）引发的隐私风险的安全措施。

请注意，上述列举的组织和技术措施是保护PII各项措施中的一部分。将来还可能出现新的措施，因为这方面的研究正在进行之中。

9.8 评估RFID系统对隐私的影响

RFID服务提供商或数据控制方使用RFID系统记录或收集PII，或将RFID标签中的物体信息与PII相联系时，应在RFID系统投入使用（最好在设计阶段）前分析和评估伴随RFID系统使用带来的PII泄露的可能性和对PII造成的威胁，确保PII不会受到侵犯。

由于技术配置和使用情形不胜枚举，因此不存在适用于各种RFID应用的万全良策。有鉴于此，有关对隐私影响的评估可能有助于确定有关隐私影响（根据法律和技术等不同观点），并将帮助找到降低影响的最佳战略。以下具体说明可能的隐私影响分析流程。PIA应涵盖整个RFID系统。

– 步骤1：项目启动

该步骤旨在确定执行PIA的业务范围，组建PIA执行团队，同时应用PIA手段反应已确定的范围。

– 步骤2：数据流程分析

该步骤的目的是制做个人可识别信息的框图或流程图，以便通过确定由影响评估目标服务处理的个人可识别信息和包含此类信息的信息资产检查风险分析目标。

具体而言，在该步骤中，通过使用框图或流程图中的相关方法，确定将收集、使用、存储、处理掉或向第三方提供的PII。此外，该步骤还说明负责PII每阶段工作（收集、使用、存储和处理）工作的人员的作用和职责。

– 步骤3：分析个人可识别信息受到侵犯的因素和风险

该步骤旨在确定对个人可识别信息资产造成的威胁和存在的薄弱环节，并据此进行风险分析。

– 步骤4：改善计划和风险管理规划

该步骤的目的是，根据对个人可识别信息进行的各种风险分析，确定需得到管理的风险程度，并为每一种将得到减缓和管理的风险制定各种控制方法。

– 步骤5：报告PIA结果

该步骤是PIA流程中最为关键的步骤之一，涉及制定和提交有关PIA流程和结果的报告。

PIA报告应包括PIA所有流程中讨论内容的结果，从PIA结果到有关个人可识别信息的已确定风险的控制和风险管理方法等。

请注意，上述PIA流程仅仅是一个演示，实际的PIA流程可经调整满足具体需求或基于其它现有的外部PIA流程。

9.9 指定数据保护官员

数据控制方应指定数据保护官员，特别负责保留一个登记册，包含有关数据控制方详尽的处理操作，其中包括有关隐私影响评估的信息和RFID应用的安全措施，以便尽快处理用户投诉及其提出的行使权力的要求。

附录 I

RFID标签的特性和限制

（本附录不构成本建议书的组成部分）

I.1 RFID标签的分类和特性

本节阐述RFID标签的分类和特性，并说明为何无法轻易在无源标签中使用安全技术。通常RFID标签被分为无源和有源标签两个类别。表I.1所示为标签分类。

表I.1 – RFID标签分类和特性

特性	无源标签	有源标签
电源	由识读器供电	内部电池
通信距离	3米或更短	100米或更长
寿命	无限制	受电池寿命限制
数据存储	识读/写入数据存储量小（字节）	识读/写入数据存储量大（k字节）
典型应用	库存管理、零售、行李/集装架控制、安全卡等	带有个人跟踪的复杂应用等（医疗卫生或地点监测，公路收费等）

无源标签没有内部电源，它们利用RFID识读器传送的电力向识读器发送信号。无源标签的通信距离为3米或更短。在13.56 MHz情况下，通信距离约为4~10厘米，但使用大型天线可将此距离加大到约70厘米。UHF标签具有更长的通信距离，约为3米~7米。

与无源标签不同，有源标签具备自身电源，使其能够自身向识读器发送信号。有源标签的通信距离约为100米或更长，但其寿命受到电池寿命的局限。此外，有源标签比无源标签更大，更昂贵。

通常，在（125/135 kHz）频率之下或（13.56 MHz）频率之上工作的系统为无源系统。在特高频（433/900 MHz，2.45 GHz）和微波频段内工作的系统可以是无源系统，也可以是有源系统。

低频率标签由于扫描距离短，因此最常用于安全、资产管理和产品真伪检查等方面；高频率标签由于扫描距离在30米以上，因此往往用于铁路服务、物流和配送领域。尤其值得指出的是，13.56 MHz标签被纳入和使用于信用卡或交通付费卡中。此外13.56 MHz系统还被用于电子护照和近场通信（NFC）。

I.2 无源标签的限制

许多RFID行业的专家指出，RFID标签的价格应低于5分，以促进RFID市场的发展。这种有关RFID标签价格的要求限制了标签可使用的资源，如电力、处理时间、存储空间和门的数量。

低于5分的RFID标签只能存储几百比特数据，拥有5-10 K逻辑门，且最大通信距离仅为几米。如果门数为上述数量，则仅有250至3000门可专用于安全功能。此外，也应将功率限制考虑在内，因为目前多数RFID标签为无源标签。

立法往往还限制识读器的辐射功率，因此，标签功率受到限制。在现今技术条件下，即使没有成本限制将安全的标准加密技术用于无源标签仅限于短距离标签。在通信距离为若干米的标签中，识读器辐射的功率不足以为实施安全加密功能所需的诸多门提供功率。

按照[b-CRYPTREC]，需要6~13 K门来实施非对称加密算法，同时需要类似数量的门来实施散列功能。例如，需要20~30 K门才能标准地实施先进加密标准（AES）。目前，正在开发用于RFID标签的轻型加密算法。即便如此，由于这些有关资源的限制，目前尚未完全在标签中实施加密算法。

附录 II

保护RFID系统中PII的技术措施

（本附录不构成本建议书的组成部分）

目前正在开发各种不同PII保护技术，以最大限度地减少RFID应用服务中对隐私的侵犯。特别应当指出，目前正在开发下述新技术，因为现有隐私保护的加密和认证技术由于RFID标签存在的资源限制而无法得到使用。

II.1 使用口令的灭活标签

该技术是最为常用的保护用户隐私的方法，主要利用RFID标签具有“灭活”或“有源”阶段的性质。需要时，识读器发送包括口令（32位）在内的“灭活”命令终止标签功能。然而，“灭活”标签仅适用于某些应用，因为一旦采用“灭活”命令，则无法再使用作为RFID技术优势之一的自动识别功能。例如，如果在购买时终止了附着于RFID标签的项目标签功能，则无法退换该产品，因为已无法追溯所述产品的历史。此外，“灭活”标签也不具备足够的安全性来保护PII，因为它仅拥有一个32位的口令，且“灭活”功能很可能受到拒绝服务攻击的影响（在此类攻击中，攻击者对其周围的所有标签进行灭活）。

II.2 应用物理技术保护隐私

II.2.1 法拉第笼

法拉第笼这一技术防止非法RFID识读器对标签信息进行扫描，它采用以特殊材料制成的、阻断无线电发射的容器来干扰识读器的无线信号传输，具体采用金属绕线来封锁无线信号。然而，尽管该技术在某些领域中极为有益，但法拉第笼的使用相对有限，因为当项目从容器上取掉后，就失去了隐私保护功能。

图 II.1 – 法拉第笼密码钱包

II.2.2 封锁标签

封锁标签由RSA于2003年开发。该特殊RFID标签可以防止由于非法识读器企图干扰邻近标签通信（通过生成无意义信号实现）而使标签信息泄露的情况。例如，RFID标签包含一个被指定为“公共”或“私人”的比特。对于附着有这一标签的医疗供应品而言，该特殊比特在出售前被设定为“公共”，而在用户在柜台上购买时则被改变为“私人”。如果将带有“私人”标签的医疗供应品插入带有封锁标签的容器，则由封锁标签设定为“私人”的标签的标签信息无法由其他人识读，因此保护了购买者的隐私。

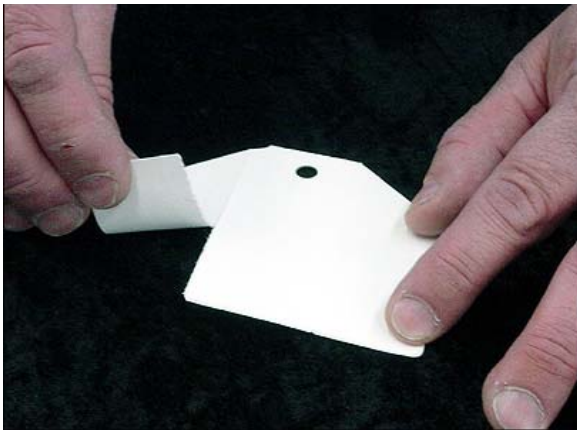
II.2.3 有源干扰

有源干扰干扰装置附近的所有RFID识读器的操作，具体采用可发出强烈干扰电波的装置实现。该技术通过该方法封锁RFID标签信息，从而保护个人信息免遭泄露。

请注意，封锁标签和有源干扰都是简单的技术，轻而易举地便可用于拒绝服务攻击。此外，这些是仅可用于用户层面可行解决方案，但不能纳入RFID服务。

II.2.4 消波标签

消波标签由IBM公司开发，旨在弥补“灭活”口令的不足，具体做法是切断标签内的某些天线连接线，从而缩短标签的通信距离。该技术可最大限度地降低通过远程地点追踪进行的隐私侵犯，因为它在保持标签信息存储功能不变的条件下，大大缩短信息的距离。



X.1275(10)_FII.2

图 II.2 – 消波标签

II.2.5 RFID灭杀器

RFID灭杀器是2005年Chaos通信大会提出的。该电子装置可永远中止无源RFID标签的活动。RFID灭杀器旨在不对RFID标签所附属的任何装置造成破坏，与有源干扰和消波标签等其它方法完全不同。

II.3 利用加密技术保护隐私

以下解决方案使用轻型加密协议在标签层面提供更好的安全性和隐私保护。所建议的解决方案尚不成熟无法在实际应用当中得到有效使用，但学术界对此已开展了很多研究。尽管今天尚不得应用，所建议的解决方案对人们了解未来成熟的解决方案提供了重要的启发。请注意，这些协议很可能需要改变现有标准化无线电协议（[b-ISO/IEC 14443]、[ISO/IEC 18000] 或EPCGlobal内进行的研究）。

II.3.1 散列锁

散列锁是典型的采用加密技术的方法之一，它将标签信息传送至得到授权的识读器和后端数据库，其唯一的基础是计算单向散列函数的反向函数的困难程度。如图II.3详细所述，只根据识读器标签信息的要求提供metaID，之后，在检查识读器是从后端数据库合法得到认证信息后才对其进行发送。然而，该方法也带来一个问题，即无法跟踪用户，因为metaID是一个静止值，而且可能已被用作标签识别符。

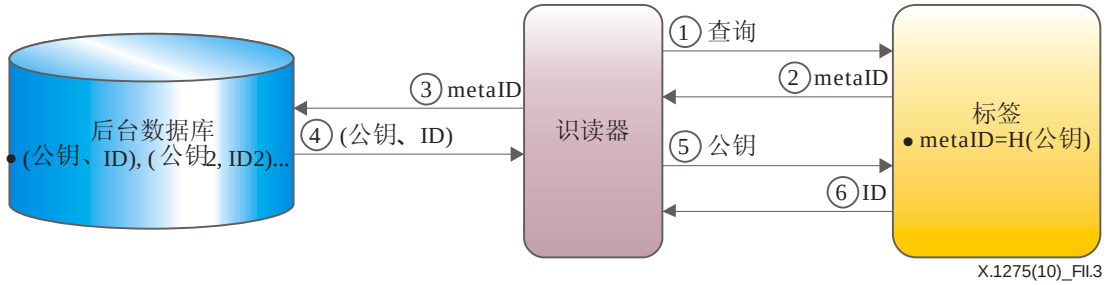


图 II.3 – 散列锁

建议采用随机散列锁技术解决现有散列锁技术中的用户跟踪问题。如图II.4详细所述，该技术通过迫使标签在标签信息被访问时产生不同数值（利用带有散列函数的随机号码生成器）而防止跟踪。目前也提出了关于其它各种不同基于散列函数（如散列链）的技术的建议，但这些技术均被认为不切合实际[b-Weis]。

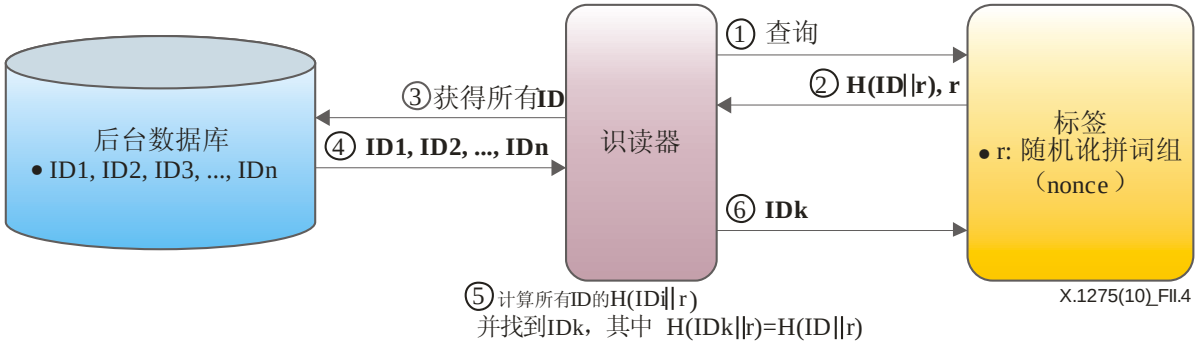


图 II.4 – 随机散列锁

II.3.2 再加密

再加密方法只允许带有后台数据库公钥的后台数据库或识读器收集标签信息，因为合法后台数据库或识读器利用公钥定期对标签身份进行加密，并在标签中保存所生成的信息，再加密协议基于ELGamal，分为两步。首先，后台数据库使用公钥和随机号码生成C，然后将C存入标签。第二步详情见图II.5。

该方法可用于高价值说明（note）。一旦采用该方法，则定期加密即防止对RFID标签信息的跟踪。然而，通过在公钥传输过程中进行线路窃听还是可能造成信息泄露的威胁，因为在此使用了公钥加密方法。此外，基于公钥加密的方法（如再加密）无法应用于采用现有可用技术的低价格无源标签中。

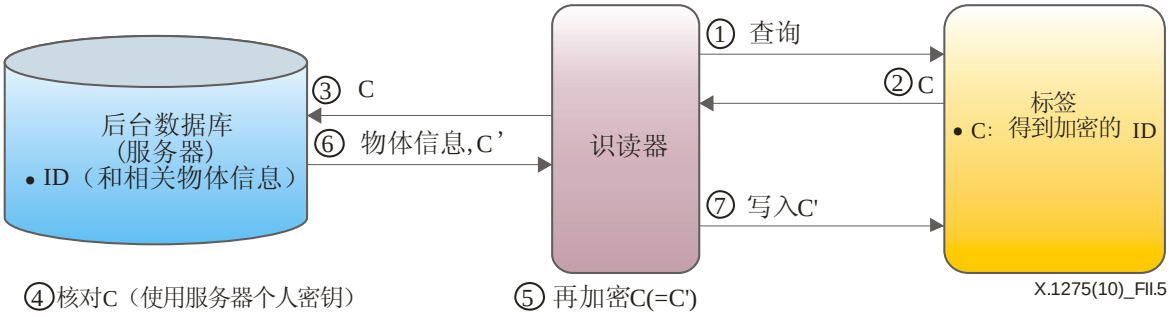


图 II.5 – 再加密

参考资料

[b-Council of Europe] Council of Europe, "*Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data*", 1981. http://conventions.coe.int/Treaty/EN/Treaties/Html/108.htm

[b-CRYPTREC] Telecommunications Advancement Organization of Japan, "*CRYPTREC Report 2002*", March 2003, Information-technology Promotion Agency, Japan.

[b-DSTI/ICCP] "*RFID, OECD Policy Guidance, A Focus on Information Security and Privacy, Applications, Impacts and Country Initiatives*", OECD Ministerial Meeting on the Future of the Internet Economy, Seoul, Korea, 17-18 June 2008.

[b-EC1] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, Official Journal L 281, 1995. http://ec.europa.eu/justice_home/fsj/privacy/docs/95-46-ce/dir1995-46_part1_en.pdf

[b-EC2] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications). http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32002L0058:EN:HTML

[b-EPIC] Electronic Privacy Information Center, "*Guidelines on Commercial Use of RFID Technology*", July 2004.

[b-E-Zpass] http://www.ezpass.com/static/info/howit.shtml

[b-ICAO] ICAO, Doc 9303, *Machine Readable Travel Documents*, Part 1, Volume 2, 6th edition, 2006.

[b-IPC] Information and Privacy Commissioner/Ontario, "*Privacy Guidelines for RFID information Systems (RFID Privacy Guidelines)* ", June 2006.

[b-Isamu Y] Isamu, Y., Shinichi, S., Akira, I. and Satoshi, I., "*Secure Active RFID Tag System"*, 7th International Conference on Ubiquitous Computing, September 2005.

[b-ISO 22307] ISO 22307:2008, "*Financial services – Privacy impact assessment*", August 2008.

[b-ISO/IEC 14443] ISO/IEC 14443:2008, Identification cards – Contactless integrated circuit cards – Proximity cards.

[b-Japan] MIC (Ministry of Internal Affairs and Communications), METI (Ministry of Economy, Trade and Industry) Government of Japan, "*Guidelines for Privacy Protection with Regard to RFID Tags*", July 2004.

[b-Juels] Juels, A., Rivest, R.L., and Szydlo, M., "*The Blocker Tag: Selective Blocking of RFID Tags for Consumer Privacy*", ACM Conference on Computer and Communications Security, 2003.

[b-Junichiro] Junichiro Saito, Jae-Cheol Ryou, and Kouichi Sakurai, "*Enhancing privacy of Universal Re-encryption scheme for RFID tags*", Embedded and Ubiquitous Computing 2004.

[b-Korea] MIC (Ministry of Information and Communication) of Korea, "*RFID Privacy Protection Guideline*", July 2005.

[b-NIST] NIST SP 800-98, "*Guidance for Securing Radio Frequency Identification (RFID) Systems*", September 2007.

[b-OECD] OECD, "*Guideline on the Protection of Privacy and Transborder Flows of Personal Data*", 1980.

[b-Peris-Lopez] Pedro Peris-Lopez *et al*, "*M^2 AP: A Minimalist Mutual-Authentication Protocol for Low-cost RFID Tags*", 3rd International Conference on Ubiquitous Intelligence and Computing, September 2006.

[b-PIA Canada] Treasury Board of Canada Secretariat, "*Privacy Impact Assessment Guidelines: A Framework to Manage Privacy Risks*", 2002.
http://www.tbs-sct.gc.ca/pubs_pol/ciopubs/pia-pefr/paipg-pefrld2-eng.asp

[b-PIA Korea] MIC (Ministry of Information and Communication) of Korea, "*Privacy Impact Assessment Guideline for Private Sector*", December 2005.

[b-Simon L1] Simson, L., Garfinkel, Ari Juels, and Ravi Pappu, "*RFID Privacy: An Overview of Problems and Proposed Solutions*", IEEE Security and Privacy, 2005.

[b-Simon L2] Simson, L., Garfinkel and Beth Rosenberg, "*RFID: Applications, Security, and Privacy*", Addison-Wesley Professional, July 2005.

[b-UNHCR] UN General Assembly, "*Guidelines for the Regulation of Computerized Personal Data Files*", 1990.
http://daccess-dds-ny.un.org/doc/UNDOC/GEN/G90/107/08, PDF/G9010708-pdf

[b-Weis] Weis S., *et al.*, "*Security and Privacy Aspects of Low-Cost Radio Frequency Identification Systems*", Security and Pervasive Computing 2003.

ITU-T系列建议书

A系列	ITU-T工作的组织
D系列	一般资费原则
E系列	综合网络运行、电话业务、业务运行和人为因素
F系列	非话电信业务
G系列	传输系统和媒质、数字系统和网络
H系列	视听及多媒体系统
I系列	综合业务数字网
J系列	有线网络和电视、声音节目及其它多媒体信号的传输
K系列	干扰的防护
L系列	电缆和外部设备其它组件的结构、安装和保护
M系列	电信管理，包括TMN和网络维护
N系列	维护：国际声音节目和电视传输电路
O系列	测量设备的技术规范
P系列	电话传输质量、电话设施及本地线路网络
Q系列	交换和信令
R系列	电报传输
S系列	电报业务终端设备
T系列	远程信息处理业务的终端设备
U系列	电报交换
V系列	电话网上的数据通信
X系列	**数据网、开放系统通信和安全性**
Y系列	全球信息基础设施、互联网协议问题和下一代网络
Z系列	用于电信系统的语言和一般软件问题

瑞士印刷
2011年，日内瓦