国 际 电 信 联 盟

ITU-T X.1171

(02/2009)

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

安全应用和服务 – 网络身份安全

在采用基于标签识别的应用中对保护个人可识别信息的威胁和要求

ITU-T X.1171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

欲了解更详细信息，请查阅ITU-T建议书目录。

ITU-T X.1171建议书

在采用基于标签识别的应用中对保护个人可识别信息的威胁和要求

摘要

无线射频识别（RFID）等识别标签的广泛部署可能带来隐私受到侵害的问题，由于RFID技术能够自动采集（处理）数据，就可能将此数据向公众公开（故意或意外）。

在个性化售后管理应用、医疗保健相关应用等应用中，对于采用基于标签识别以及依赖个性识别标签的应用，隐私问题正在成为一个日益严重的问题。本建议书描述采用基于标签识别的应用的一些个人可识别的信息（PII）侵害以及对PII保护的要求。另外，本建议书基于PII政策轮廓提供了PII保护的基本结构。

来源

ITU-T第17研究组（2009-2012年）按照世界电信标准化全会（WTSA）第1号决议规定的程序，于2009年2月20日批准了ITU-T X.1171建议书。

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.1171 建议书[1]

在采用基于标签识别的应用中对保护PII的威胁和要求

1 范围

本建议书涉及在采用基于标签识别的应用中对保护PII的威胁和要求等问题，描述如下：

– 描述在基于企业对客户（B2C）环境中，采用基于标签识别的应用对PII的威胁；

– 确定在基于企业对客户（B2C）环境中，采用基于标签识别的应用对PII保护的要求。

本建议书不涉及下列问题：

– 分析采用基于标签识别的应用的一般安全威胁和要求；

– 分析识别（ID）标签和ID终端之间PII威胁和要求；

– 分析取决于特定ID标签和读取方法的PII威胁和要求；例如，无线电频率识别（RFID）标签和ID终端；

– 根据采用基于标签识别的应用的用户PII政策轮廓，规定和开发PII保护的消息格式和机制。

注1 – 未来的工作将是定义此格式，它可能不限于基于标签识别使用的PII唯一的保护，而是可能有更加通用的（私人）方法。

本建议书中，ID标签用户有控制ID标签的能力，因此，假设ID标签用户负责ID标签的行为。

注2 – 在某些情况下，ID标签用户不能拥有控制ID标签的所有能力。例如，某个用户购买了被标记的产品，制造商要求出于保修目的保持ID标签起作用。在此情况下，ID标签用户可能只是携带和使用被标记的产品的用户。因此，本建议书不适用于解决此类情况下的上述问题。此情况涉及立法和政策问题（参见[b-OECD]），此类问题可能在另一个建议书中规定。

2 参考文献

下列ITU-T建议书和其他参考文献的条款，通过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。所有的建议书和其他参考文献都面临修订，使用本建议书的各方应探讨使用下列建议书和其他参考文献最新版本的可能性。当前有效的ITU-T建议书清单定期出版。在本建议书中对另一个文件的参引，并不意味着作为一个单独文件，给予其建议书的地位。

[ITU-T X.1121] ITU-T X.1121建议书（2004），《移动端到端数据通信的安全技术框架》。

[1] 根据德国的法律，本建议书可能不适用于德国。

3 定义

3.1 其他资料规定的术语

本建议书采用其他资料规定的术语：

3.1.1 access control [b-ITU-T X.800] **访问控制**：防止未被授权地使用资源，包括防止以未被授权的方式使用资源。

3.1.2 application server [ITU-T X.1121] **应用服务器**：连接到开放网络的实体，与移动终端进行数据通信。

3.1.3 application service provider (ASP) [ITU-T X.1121] **应用服务提供商**：一个实体（个人或组织），通过应用服务器向移动终端用户提供应用服务。

3.1.4 authentication [b-ITU-T X.811] **认证**：保证实体要求的身份的规定。

注 – 身份一词在电信环境下的使用理解为：它是可信的一个标识符或标识符组，经过确认过程之后，在特定情况下表示一个网络单元、网络终端设备或用户是可靠的。但此处使用本术语时，不能断定可信的标识符构成对一个人的肯定证实。

3.1.5 identifier [b-ITU-T F.771] **标识符**：用以识别现实世界中的实体所采用的一串数字、字符和符号或任何其他形式的数据。它代表现实世界中的实体和其在计算机中信息/属性之间关系。该关系能使用户通过用户的ID终端访问计算机中存储的实体的信息/属性。

3.1.6 ID tag [b-ITU-T F.771] **ID 标签**：一个存储少量信息的微小的物体，可以是一个标识符或包括一个标识符和其他附加应用数据如姓名、标题、价格和地址。

3.1.7 ID terminal [b-ITU-T F.771] **ID终端**：一种设备，具有从ID标签采集数据能力以及其他能力如通信能力、多媒体信息显示能力。数据采集能力可能包括从ID标签获得标识符的功能，可以没有通信能力如条形码和2D条形码。例如，利用数据采集技术设备的实例是数码相机、光学扫描器、射频转发器、红外线传输模组、电镀明线线路等。

3.1.8 mobile network [ITU-T X.1121] **移动网络**：提供到移动终端无线网络访问点的网络。

3.1.9 mobile terminal [ITU-T X.1121] **移动终端**：具有无线网络访问功能的实体，并与移动网络相连接，与应用服务器或其他移动终端进行数据通信。

3.1.10 mobile user [ITU-T X.1121] **移动用户**：使用并操作移动终端以接受应用服务器提供的各种服务的实体（个人）。

3.1.11 personally identifiable information (PII) 个人可识别信息：与任何活着的人有关、可识别此类个人的信息（包括当与其他信息结合时能够识别一个人的信息，即使该信息不能清楚地识别一个人）。

3.2 本建议书中规定的术语

本建议书规定下列术语：

3.2.1 applications using tag-based identification 采用基于标签识别的应用：至少涉及以下元素的应用：标识符、ID终端、ID标签和网络。在此应用中，标识符存储在ID标签上并且所有与标识符相关的信息均在网络侧提供。

注 – 标识符存储在ID标签上（或在ID标签中，取决于ID标签的类型），并且通过光学扫描（只读）、相机（只读）、红外（读/写）、射频技术（读/写）或其他类似的方法，ID终端从/至ID标签读取或写入标识符。

3.2.2 business-to-consumer (B2C) 企业到消费者：企业和消费者之间的一种商业关系，其中业务提供商提供有价值和有用的服务给消费者，消费者使用这些服务。

3.2.3 default PII policy profile 默认PII政策轮廓：一组采用基于标签识别应用的格式化的PII保护规则和政策。

3.2.4 identification (ID) 识别：通过**读取**ID标签的标识符，将一个物品从一大类物品中识别出来的过程。

3.2.5 ID tag user ID标签用户：购买并携带或使用带有ID标签的物品的人。

3.2.6 ID terminal user ID终端用户：使用并操作ID终端的人。ID终端用户的典型例子可以是具体ID终端的移动用户。

3.2.7 personalized ID tag 个性化ID标签：一个ID标签，所包括的标识符可以识别独特的而非匿名的物品。

3.2.8 PII protection service (PPS) 个人可识别信息保护业务：一项安全业务，对采用基于标签识别应用的ID标签和/或ID终端的用户PII提供保护。在运行基于标签识别应用的网络上，PPS管理（即创建/更新/删除/应用）（ID标签和/或ID终端）用户的PII政策轮廓。

3.2.9 PII policy profile PII政策轮廓：一组格式化的PII保护规则和政策。

3.2.10 user-defined PII policy profile 用户定义的PII政策轮廓：一组由（ID标签和/或ID终端）用户定义的格式化的PII保护规则和政策。

4 缩写词和首字母缩略语

本建议书采用下列缩写词和首字母缩略语：

ASP 应用业务提供商
B2C 企业到消费者
ID 识别
IrDA 红外数据协会
OECD 经济合作与开发组织
PII 个人可识别信息
PPS PII保护业务
RF 射频
RFID 射频识别
SCM 供应链管理

5 惯例

无。

6 概述

识别标签（包括RFID标签）的广泛部署可能带来隐私受到侵害的问题，由于RFID技术能够自动采集（处理）数据，就可能将此数据向公众公开（故意或意外）。

在个性化售后管理服务、医疗保健相关服务等应用中，对于采用基于标签识别以及依赖个性化识别标签的应用，隐私问题正在成为一个日益严重的问题。

在学术界和企业界中，大部分符合PII保护机制的行为侧重于ID标签和ID终端之间的认证协议。然而，这些行为不适用于某些实际环境，特别是采用基于标签识别的应用，在该环境下标识符的有效信息存储于网络域中的服务器上。因此，必须提出在采用基于标签识别的应用的环境下适当的PII保护机制。基于轮廓的PII保护机制可能是针对此环境的许多解决方案中的一种。

本建议书描述采用基于标签识别的应用的环境中的PII侵害，PII保护的要求，以及根据用户定义的PII政策轮廓的PII保护的基本结构。

7 采用基于标签识别的B2C应用

采用基于标签识别的应用定义为一个扩展的而且更全面的识别应用，用于与一系列的网络、内部网和全球性分布的应用系统之间的通信。换言之，基于标签识别的应用是由ID标签（包括RFID）触发的以全球网络为基础的应用。

在企业界，如供应链管理（SCM）和仓库管理以及在药品供应链的防伪措施中，已经广泛使用了采用基于标签识别的应用，目前基于标签识别的应用已经扩展到了终端用户应用领域（例如，由ID标签触发的产品信息内容交付，实物的售后管理，病人的病历，收费控制等）以及工业应用。

采用基于标签识别的B2C 应用可以分为三类：

a) 客户作为ID终端用户：例如，在信息内容交付服务中，客户使用他/她的ID终端检索信息。在此业务类型中，大部分应用业务提供商可能假定，ID终端具有移动通信能力和多媒体信息显示能力。图1示出此类基于标签识别的应用的基本模型。它由两个基本网络操作组成：ID解析和内容检索。ID解析程序是将一个标识符翻译或解析为地址[b-ITU-T Y.2213]。配备了ID终端的移动终端，首先通过目录服务解析从ID标签收到的标识符，再进行内容检索。

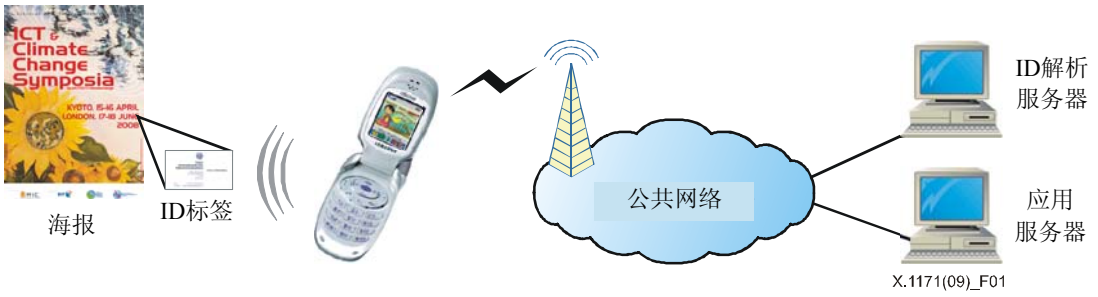

图 1 – 基于标签识别的B2C应用的基本模型

b) ID标签用户作为客户：基于标签识别的B2C应用的一个典型的实例是处理访问控制和/或认证，例如，入口检查、护照、执照、售后管理服务等。在此类应用模型中，ID终端为固定终端类型和/或移动终端类型；客户可不需要他/她自己的ID终端。

c) ID标签用户和ID终端用户双方作为客户：产品信息检索服务（基于标签识别的B2C应用的基本类型），一个客户在从他/她的移动终端浏览了产品信息内容后购买了被标记的产品的变为了一个标签用户。在另一个例子是由启用ID标签的门诊卡触发的医疗保健相关服务，在此应用中，客户的类型很多，例如，患者、医生、护士等作为ID标签用户。通过读取他/她的启用ID标签的门诊卡，ID标签用户可以通过带有ID终端的移动终端浏览他/她自己的门诊记录。

由于许多采用基于标签识别的应用扩展为B2C应用，客户非常关心通过ID标签导致的PII泄漏问题。在本建议书中，我们主要关注于采用基于标签识别的B2C应用的模型。

8 采用基于标签识别的B2C应用的参考模型

图2表示一个采用基于标签识别的B2C应用的参考模型。

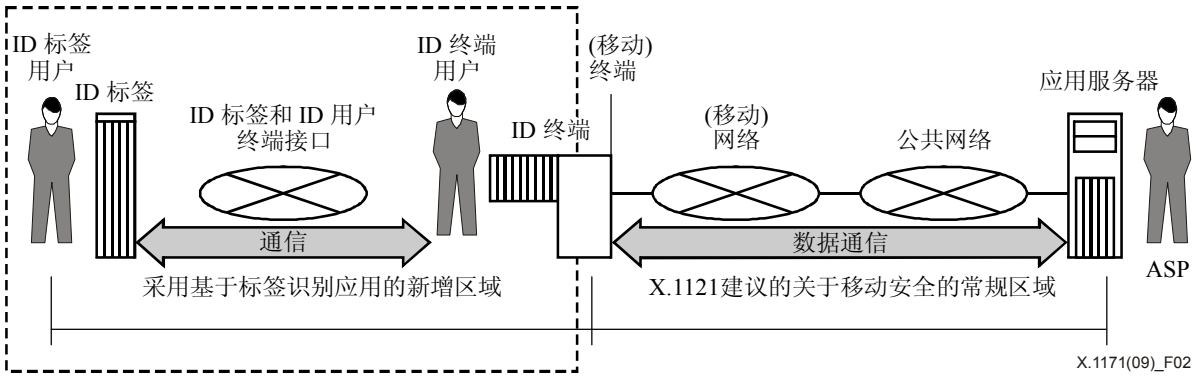

图 2 – 采用基于标签识别的B2C应用的参考模型

本参考模型是[ITU-T X.1121]中移动端到端数据通信的新增模型。新增的实体包括ID标签、ID标签用户、ID标签和ID终端接口和ID终端。在此模型中，（移动）终端可以是有线的固定终端以及无线移动终端，还可以被认为是ID终端。

9 采用基于标签识别的B2C应用中的PII侵害

在采用基于标签识别的应用环境下，主要的PII侵害出现的情况是：配备有ID标签的产品或文件的所有权转让给了私人。

在采用基于标签识别的应用环境下，可以有几种标识符存储/读取方法，如（二维）条形码和光学扫描仪（或摄像机）、近场无源RFID标签和阅读器、远场无源RFID标签和阅读器。本节只描述在采用基于标签识别的应用的基于B2C的环境下，一般PII的泄漏。对如下所述的威胁更精确的描述不包括在本建议书的范围内：

– 在采用基于标签识别的应用中的通用安全威胁：本节只关注于采用基于标签识别的应用中的PII相关的威胁。

– 标识符存储/读取方法特定的威胁：例如，在RFID标签情况下，攻击者可以通过RFID标签的标识符跟踪RFID被标记产品的ID标签用户的位置。附录一详述了RFID环境下这种定位跟踪。

– ID标签和ID终端之间的威胁：本节只关注网络侧的PII威胁。

9.1 与标识符相关信息的泄漏

攻击者可以从ID标签中读取信息而不需要了解被标记产品的ID标签用户。首先，攻击者从用户携带的ID标签中读取标识符。而后，他/她解析标识符并从目录服务中查询信息位置。最后，攻击者请求与ID标签相关的信息。此外，如果信息与PII相关，如信用卡信息、病历等，则会对ID标签用户的PII造成更为严重的侵害。图3描述了由于信息泄漏而造成的PII侵害。在此情况下，攻击者可以采集到某些动态的信息（购买被标记产品的时间和地点，跟踪产品的信息等）以及静态信息如产品名称和描述。

防止此类PII侵害的方法是，除去ID标签或使ID标签功能失效。但在许多采用基于标签识别的应用中，如个性化售后管理服务、医疗保健相关服务等，保留ID标签和其功能是必须的。

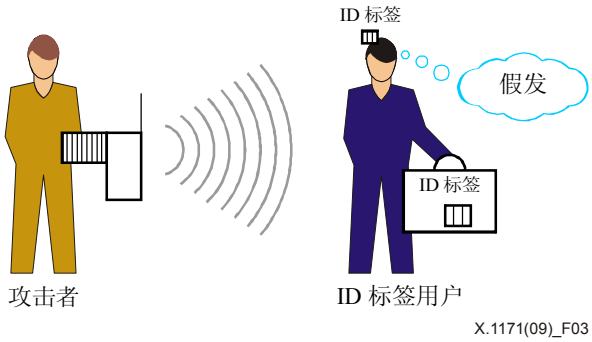

图 3 – 由于信息泄漏而造成的PII侵害

9.2 历史背景数据的泄漏

攻击者可以从与ID标签相关的历史背景数据中有目的的抽取用户信息，如偏好、习惯、感兴趣的领域等。而且，攻击者可以不经用户同意将此数据用于违法或商业目的。在此类侵害情况中，用户指ID终端用户。ID终端用户使用他/她的ID终端从被标记产品或文件读取标识符，并从采用基于标签识别的应用中的应用服务器获得有用信息。目前，通过采用基于标签识别的应用的网络，可以采集到各种背景日志数据（DVD影片的出租日、购买物品的日期和地点、阅读影片海报的地点等）；此数据可以与用户链接（参见图4）。

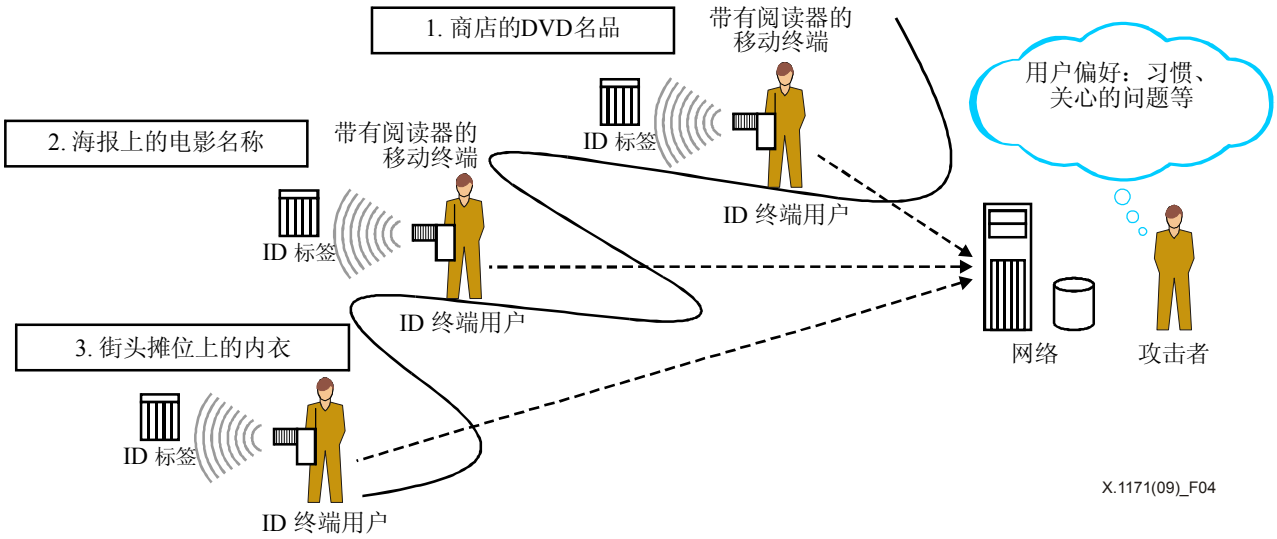

图 4 – 通过对历史背景数据的采集造成的PII侵害

9.3 PII侵害和参考模型之间的关系

表1概括了在图2中所示的模型中PII侵害和实体之间的关系。在表中，标有“X”的格子表示行中的PII侵害相关于列中的实体或实体之间的关系。

表 1 – PII 侵害和参考模型之间的关系

实体和实体之间的关系	侵害	
	采用基于标签识别的应用提供的信息泄漏	应用服务器中存储的历史背景数据泄漏
ID标签和ID终端用户之间的关系		X
（移动）终端和应用服务器之间的关系	X	X
ID标签用户和应用服务器之间的关系	X	
ID标签和应用服务器之间的关系	X	
应用服务器	X	X

10 对采用基于标签识别的B2C应用的PII保护要求

本节主要描述防止第9节分析的两类PII侵害的技术要求。RFID技术背景中，针对RFID用户和销售商的关于PII保护方面更全面的准则在其他建议书中涉及。这些要求部分基于OECD隐私准则[b-OECD]的原则。附件A描述了本条款所考虑的[b-OECD]原则，附件B描述了[b-OECD]的更多原则。从采用基于标签识别的B2C应用中的PII侵害考虑，得出下列要求：

– ID标签用户和/或ID终端用户对PII的控制；

– 对ID标签用户和/或ID终端用户的认证；
– 在应用服务器中对ID标签用户的PII的访问控制；
– ID标签相关信息的数据保密；
– 对PII的同意采集；
– 应用服务器的技术安全保护。

10.1 ID标签用户和/或ID终端用户控制PII

要求ID标签用户和/或ID终端用户在网络上能够管理或更新与他/她的ID标签和/或ID终端相关的PII。以这种方式，用户可以确定基于标签识别的应用中哪些PII应被删除或保留。此外，用户还可在采用标签识别的应用中为他/她的PII确定时间限制。

10.2 对ID标签用户和/或ID终端用户的认证

要求基于标签识别的应用的应用服务器提供ID标签用户认证程序，在必要时应用服务器可以提供ID终端用户的认证程序（某些采用基于标签识别的应用不需要认证用户）。

10.3 在应用服务器中对ID标签用户的PII的访问控制

对应用服务器所存储ID标签用户的PII的访问应是安全的且限于经授权的信息请求者并限于每个请求者所需的相关信息。

10.4 ID标签相关信息的数据保密

基于标签识别的应用的应用服务器必须提供数据保密，以保证与ID标签相关的信息不能被未被授权的使用者读取。

10.5 同意采集PII

要求基于标签识别的应用的应用服务器提供一个同意程序，以允许采集PII，包括ID终端用户相关日志数据。基于标签识别的应用提供技术解决方案，确保PII根据已明确目标的需要，保持准确和最新并限于所需的相关信息。在同意的过程中，应用应提供PII采集的目的。如果先前采集的PII要用于初始目的未包括的其他用途，需要用户另行同意。

10.6 应用服务器的技术安全保护

要求负责处理PII的基于标签识别的应用的ASP采用用于PII等应用服务器的技术安全措施。

10.7 要求和PII侵害之间的关系

表2总结了PII保护要求和PII侵害之间的关系。在表中，标有“X”表示列中的PII侵害与行中的PII保护要求相关。

表2 – 要求和 PII 侵害之间的关系

要求	侵害	
	与标识符相关 信息的泄漏	历史背景 数据泄漏
ID标签用户和/或ID终端用户控制PII	X	
对ID标签用户和/或ID终端用户的认证	X	X
在应用服务器中对ID标签用户 的PII的访问控制	X	
ID标签相关信息的数据保密	X	X
PII的同意采集		X
应用服务器的技术安全保护	X	X

附件A

国内应用的基本原则[2]

（该附件为本建议书的一个组成部分）

- 采集限制：采集个人数据应有限制且任何这样的数据应通过法定、公平和适当方式，在数据采集对象知情或同意的情况下获得。
- 数据质量：个人数据应与其使用目的相关，不超出这些目的所需的范围且准确、完整并保持最新。
- 目的明确：应在数据采集之前明确采集个人数据的目的，随后的使用应限于为了实现这些目的，或在不与这些目的相符的情况下，限于实现在每次目的变化时所明确的那些目的。
- 使用限制：如使用目的不符合已确定目的，不得披露、提供或使用个人数据。
- 安全保护：应通过合理的安全保护来保障个人数据免受丢失、非法获取、破坏、使用、修改或披露数据等风险。
- 开放：应制定与个人数据开发、实践和政策有关的通用开放政策。应具备确定个人数据的存在与属性、其使用的主要目的以及数据控制人的身份和常住地等随时可用方法。
- 个人参与：个人应有权：
  a) 从数据控制人获得数据控制人是否拥有与其相关的信息的确认；
  b) 在以下条件下，向其传送与其相关的数据
     - 在合理的时间内；
     - 缴纳一定的费用，如果有的话，不应过高；
     - 通过合理的方式；
     - 以其可以容易理解的格式；
  c) 如果根据a)和b)所提的要求被拒绝，应给予理由并可对此类拒绝提出质疑；以及
  d) 对与其相关的数据提出质疑，并在质疑成功后将数据删除、改正、完善或修正。
- 问责：数据控制人应为遵守实行上述原则的措施承担责任。

[2] 这些原则摘自于1980年经合组织（OECD）《保护隐私和个人信息跨境流动的准则》的第二部分。

附件B[3]

国际应用的基本原则：自由流动和合法限制

（该附件为本建议书的一个组成部分）

– 成员国应考虑其他成员国国内处理并再输出个人数据的影响。

– 成员国应采取一切合理及适当措施，确保个人数据的跨境流动（包括从一个成员国过境）不受中断并使其安全。

– 除非另一个成员国不实质遵守这些准则，或再输出这些数据将回避其国内隐私法规，成员国应克制对其自身和另一个成员国之间个人数据跨境流动的限制。对于其国内隐私法规因这些数据的特性而做出了具体的规定，但其他成员国未给予同等保护者，成员国也可对特定类别的个人数据加以限制。

– 成员国应避免以保护隐私和个人自由为由制定法律、政策和惯例，从而为个人数据的跨境流动制造超出此类保护要求的障碍。

[3] 这些原则摘自于1980年经合组织（OECD）《保护隐私和个人信息跨境流动的准则》的第三部分。

附录一

RFID业务中通过标识符定位跟踪

（本附录不是本建议书的组成部分）

攻击者可以通过RFID标签的标识符跟踪被标记产品的ID标签用户的位置。此类安全侵害可能通过采用无形的RFID阅读器对特定标签标识符进行跟踪或监视实现。因为攻击者可以使用标签的标识符作为个人标识符，他/她可以容易地跟踪用户的位置，如图I.1所示。

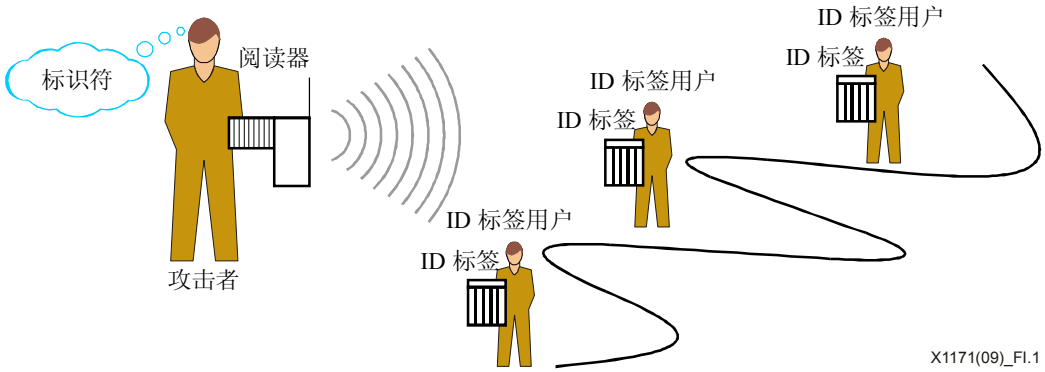

图 I.1 – 通过对私人的定位跟踪造成的安全威胁

为了对标识符进行跟踪保护，可以在RFID标签和阅读器之间采用一种认证方法。如果阅读器通过RFID标签认证，则RFID标签允许阅读器读取其标识符。换言之，没有通过认证程序，攻击者不能得到标签的标识符。然而，如果RFID标签没有足够的能力处理精深的运算，如加密运算，则此认证方法所得出的答案可能不切实际。

另一种解决方案可以是标识符重新编码技术。标识符重新编码包括RFID标签的标识符周期性重新编码，采用伪标识符（或元标识符）；因此降低了ID标签的标识符和ID标签用户之间的连接性。注意，如果RFID标签具有非重写功能或如果ID标签使用特殊的标识符格式（如EPC代码[b-EPCglobal]），则此标识符重新编码方法不适用。此外，此技术的有效性只限于需要时常阅读RFID 标签的业务，并且可能增加了服务器侧的复杂程度。

附录二

采用基于标签识别的应用的PII保护业务（PPS）

（本附录不是本建议书的组成部分）

II.1 采用基于标签识别的应用的PII保护业务（PPS）

PPS是基于用户PII政策轮廓的PII保护业务的一个例子。

第II.3节表示用于基于标签识别的应用的PPS的普通业务情况。对于PPS，特定的基于标签识别的应用使用的ID标签或ID终端用户创建适合该应用的他/她的PII保护政策，并发送到可信的第三方系统（PPS系统）。然后，本系统创建用户的PII政策轮廓并将它发送到应用服务器（业务侧系统）。此时，应用服务器可以控制访问与ID标签和/或ID终端用户相关的PII信息。

II.2 采用基于标签识别的应用的PPS的业务实体

PPS具有以下三种业务实体（参见图II.1）：

– PPS系统：作为具有用户的PII政策的管理功能的实体，创建用户定义的用户PII政策的PII政策轮廓，并向业务侧系统提供PII政策轮廓。

注 – 在负责许多采用基于标签识别的应用的集中PPS系统情况下，应提供应对单点故障的防范措施。然而，根据用户情况，可能只有一种PPS系统用于基于标签识别的应用。

– 业务侧系统：提供与ID标签的标识符相关信息的实体，即，可作为基于标签识别的应用中的应用服务器。因此，对于基于标签识别的应用可以存在许多业务侧系统。本实体提供采用用户定义的PII政策轮廓或默认PII政策轮廓的访问控制功能。

– 用户侧系统：具有无线（或有线）网络访问功能和标识符获取功能，如必须，此实体可以是带有ID终端的移动终端。ID标签和/或ID终端用户可以通过此用户侧系统访问业务侧和PPS系统。采用用户侧系统，用户控制他/她的基于标签识别的应用的PII保护政策。

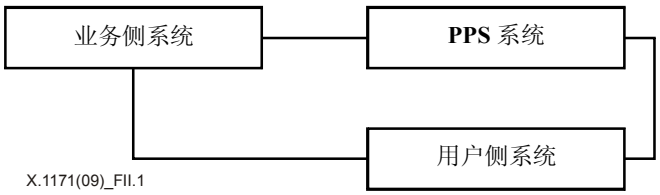

图 II.1 – 采用基于标签识别的应用的PPS的业务实体

II.3 PPS的一般服务方案

PPS的服务方案一般是从标签个性化程序如被标记的产品购买开始的。图II.2表示了基于标签识别的应用的一般PPS流程。

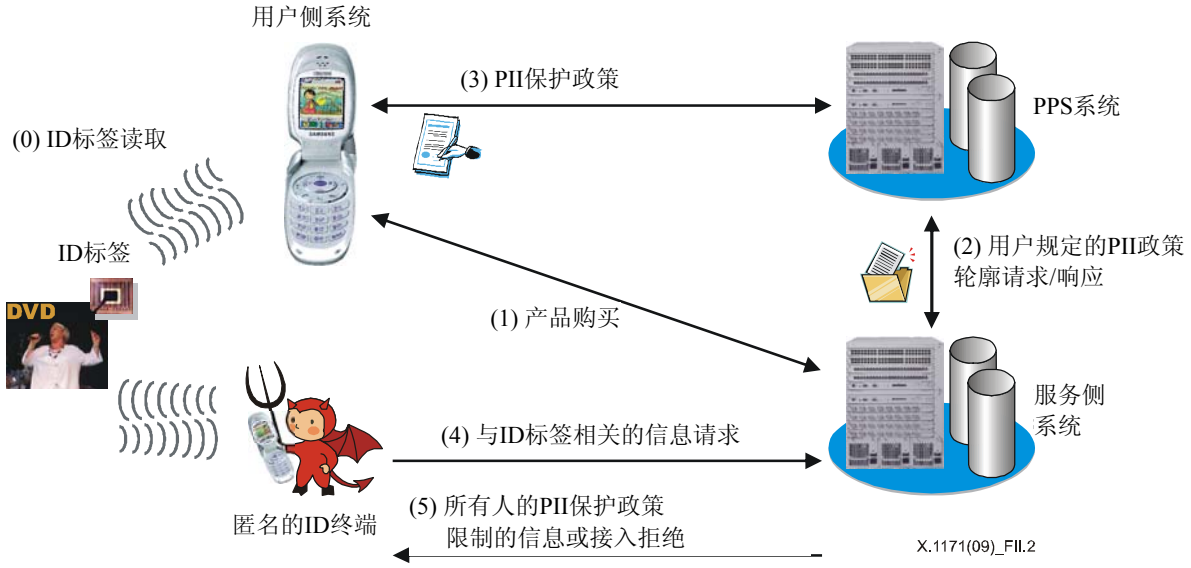

图 II.2 – 一般PPS流程

0) 客户使用他/她的备有ID终端的移动终端从被标记产品中读取标识符。

1) 客户从应用业务网络上浏览与产品相关的信息并随后采用各种支付方法中的一种购买产品。此刻，客户变成了ID标签用户。

2) 基于标签识别的应用从PPS系统请求用户定义的PII政策轮廓，然后以用户定义的PII轮廓对应用做出响应。

3) PPS系统收到本应用的用户PII保护。

4) 任何人均可以从业务侧系统请求与此ID标签相关的信息。

5) 如是请求者是ID标签用户，则请求者可以浏览由业务侧系统提供的所有信息。否则，请求者可以得到有限的信息或他/她不能得到任何信息。

注 – 未来研究PPS使用基于标签识别的应用是很有必要的，它可以反映出PPS的优势。

II.4 PPS的功能

为了满足采用基于标签识别应用的PII保护的要求，PPS有以下功能：

– PII政策轮廓管理。

– 访问控制。

– 登记。

– PII政策轮廓发送。

– PII政策轮廓刷新。

II.4.1 PII政策轮廓管理

PII政策轮廓管理是PPS的核心功能。PPS系统管理的两类PII政策轮廓描述如下：

– 默认的PII政策轮廓：表示基于标签识别的应用的一组格式化的PII保护规则和政策。这些规则可以依据正确的信息实践，如关于隐私和个人资料的跨界流动中的OECD准则（[b-OECD]）中所描述的情况。

– 用户定义的PII政策轮廓：这属于由ID标签和/或ID终端用户定义的一组格式化的PII保护规则和政策。

PPS系统执行用户定义的（或默认的）PII政策轮廓的建立和管理。确切地讲，从登记程序提供的用户PII保护政策，PPS系统应为基于标签识别的应用创建和管理默认PII政策轮廓和用户定义的PII轮廓。因此，本PII政策轮廓可以发送到业务侧系统。它基本上可以包括下列项目：

– 信息资源的公开政策（包括PII）

– 终止信息资源的政策

– 事件日志采集的政策

业务侧系统采用此PII政策轮廓对每个信息请求者的信息访问进行控制。

II.4.2 访问控制

PPS系统的访问控制功能用于认证用户或ASP的身份并准许访问用户的信息资源，主要指所有者的PII保护政策。

注 – 身份一词在电信环境下的使用理解为：它是可信的一个标识符或标识符组，经过确认过程之后，在特定情况下表示一个网络单元、网络终端设备或用户是可靠的。当此处使用本术语时，不能断定可信的标识符构成一个人的肯定证实。

换言之，业务侧系统的访问控制功能是PPS的重要成分，因为业务侧系统应控制对所有信息的访问，并提供根据用户定义的PII政策轮廓（或在缺少用户定义的PII政策轮廓时采用默认PII政策轮廓）提供PII。如是请求者已经根据所有者定义的PII政策轮廓访问了某用户的PII，则要求业务侧系统能够推断。

II.4.3 登记

业务侧系统和用户侧系统具有PPS系统登记程序，在登记程序中，由业务侧和用户侧系统提供的信息如下：

– 业务侧系统：身份信息（包括认证信息如密码）和信息类型（即价格信息、购买方法等），由应用服务器使用基于标签识别提供给用户侧系统。

– 用户侧系统：身份信息（包括认证信息如密码）和用户自己的PII保护政策和允许基于标签识别的应用。

PPS系统应为业务侧系统创建默认PII政策轮廓，并向业务侧系统提供默认PII政策轮廓（参见图II.3）。默认PII政策轮廓可以通过PII轮廓管理功能创建。

换言之，PPS系统应根据用户的PII保护政策创建用户定义的PII政策轮廓。图II.3表示PPS的登记程序。

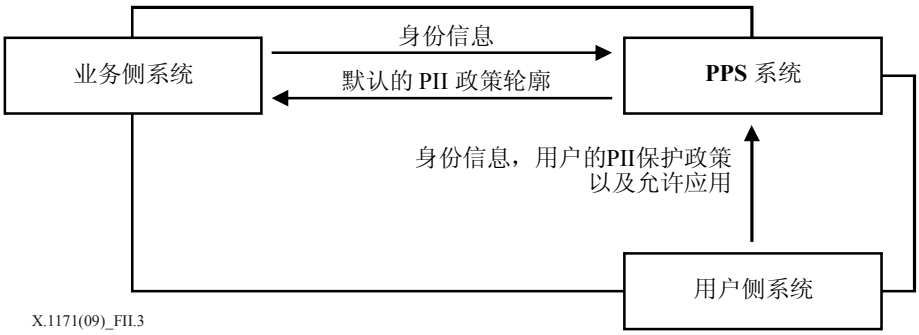

图 II.3 – 登记程序

II.4.4 PII政策轮廓发送

PII政策轮廓发送程序由业务侧系统启动。图II.4表示PII轮廓发送程序。

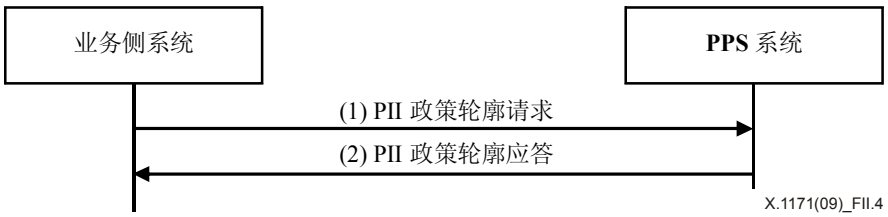

图 II.4 – PII政策轮廓发送程序

1) PII政策轮廓请求：业务侧系统请求带有用户身份的用户定义的PII政策轮廓。

2) PII政策轮廓应答：PPS系统检查该用户的用户定义的PII政策轮廓并发送用户定义的PII政策轮廓。

注 – 身份一词在电信环境下的使用理解为：它是可信的一个标识符或标识符组，经过确认过程之后，在特定情况下表示一个网络单元、网络终端设备或用户是可靠的。当此处使用本术语时，不能断定可信的标识符构成一个人的肯定证实。

II.4.5 PII政策轮廓刷新

PII政策轮廓刷新程序由PPS系统启动。当用户改变他/她自己的PII保护政策时，PPS系统再生其用户定义的PII政策轮廓。PPS系统再将PII政策轮廓刷新消息发送到所有在PPS系统中登记的业务侧系统。然后，每个业务侧系统更新用户定义的PII政策轮廓并发送PII政策轮廓刷新应答消息。图II.5表示PII政策轮廓刷新程序。

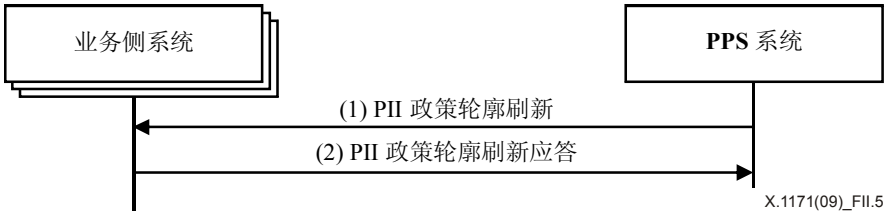

图 III.5 – PII政策轮廓刷新程序

1) PII政策轮廓刷新：PPS系统将更新的用户定义的PII轮廓发送到每个业务侧系统。

2) PII政策轮廓刷新应答：每个业务侧系统发送刷新应答消息到PPS系统。

参考资料

[b-ITU-T F.771] ITU-T F.771建议书(2008)，《基于标签识别启动的多媒体信息访问的业务描述和请求》

[b-ITU-T X.800] ITU-T X.800建议书(1991)，《*CCITT*应用的开放系统互连的安全体系结构》

[b-ITU-T X.811] ITU-T X.811建议书(1995) | ISO/IEC 10181-2:1996，《信息技术 – 开放系统互连 – 开放系统的安全框架：认证框架》

[b-ITU-T Y.2091] ITU-T Y.2091建议书(2008)，《下一代网络的术语和定义》

[b-ITU-T Y.2213] ITU-T Y.2213建议书(2008)，《采用基于标签识别应用和服务的网络问题的*NGN*业务要求和能力》

[b-ITU-T Y.2720] ITU-T Y.2720建议书(2009)，《*NGN*身份管理框架》

[b-EPCglobal] EPC全球标准(2008)，《*EPC*全球标签数据标准版本 1.4》 <http://www.epcglobalinc.org/standards/tds/tds_1_4-standard-20080611.pdf>

[b-OECD] OECD (1980)，《保护隐私和个人信息跨境流动的准则》。 <http://www.oecdbookshop.org/oecd/display.asp?CID=&LANG=EN&SF1=DI&ST1=5LMQCR2K94S8>

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
2010年，日内瓦