学校编码：10384　　分类号_____密级_____

学　　号：23020081153207　　UDC_____

厦门大学

硕　士　学　位　论　文

基于无证书密码体制的安全 EPCglobal 体系架构

Certificateless-Based Secure EPCglobal Architecture Framework

张炜道

指导教师姓名：黎 忠 文　教授

专　业 名 称：计算机系统结构

论文提交日期：2011 年　5　月

论文答辩时间：2011 年　6　月

学位授予日期：2011 年　　月

答辩委员会主席：_____

评　　阅　　人：_____

2011 年 6 月

厦门大学学位论文原创性声明

本人呈交的学位论文是本人在导师指导下,独立完成的研究成果。本人在论文写作中参考其他个人或集体已经发表的研究成果，均在文中以适当方式明确标明，并符合法律规范和《厦门大学研究生学术活动规范（试行）》。

另外，该学位论文为（　　）课题（组）的研究成果，获得（　　）课题（组）经费或实验室的资助，在（　　）实验室完成。（请在以上括号内填写课题或课题组负责人或实验室名称，未有此项声明内容的，可以不作特别声明。）

声明人（签名）：

年　　月　　日

厦门大学学位论文著作权使用声明

本人同意厦门大学根据《中华人民共和国学位条例暂行实施办法》等规定保留和使用此学位论文，并向主管部门或其指定机构送交学位论文（包括纸质版和电子版），允许学位论文进入厦门大学图书馆及其数据库被查阅、借阅。本人同意厦门大学将学位论文加入全国博士、硕士学位论文共建单位数据库进行检索，将学位论文的标题和摘要汇编出版，采用影印、缩印或者其它方式合理复制学位论文。

本学位论文属于：

（　　）1.经厦门大学保密委员会审查核定的保密学位论文，于　　年　　月　　日解密，解密后适用上述授权。

（　　）2.不保密，适用上述授权。

（请在以上相应括号内打“√”或填上相应内容。保密学位论文应是已经厦门大学保密委员会审定过的学位论文，未经厦门大学保密委员会审定的学位论文均为公开学位论文。此声明栏不填写的，默认为公开学位论文，均适用上述授权。）

声明人（签名）：

年　　月

摘 要

Al-Riyami 和 Perterson 在 2003 年的亚洲密码学会议上，提出了无证书公钥密码体制，该体制既无传统的基于证书的公钥密码体制复杂的证书管理问题又无基于身份的公钥密码体制的密钥托管问题。

EPC（电子产品代码）网络是一套先进的、综合性的复杂系统，其最终目标是为全世界的每件物品建立一套全球的、开放的标识体系，EPCglobal 是由国际物品编码协会（EAN）和美国统一代码委员会（UCC）两大标准化组织联合成立，旨在在全球范围内的各个行业推动和发展 EPC 网络，通过发展和管理 EPC 网络标准来提高供应链上贸易单元信息的透明度与可视性，以此来提高全球供应链的运作效率。

EPCglobal 体系架构在实际应用过程中存在三大安全区域：标签与阅读器构成的安全区域、ONS 查询过程构成的安全域、DNS 查询过程构成的安全域。因此利用无证书密码体制的优点，增强 EPCglobal 系统的安全性，对推动全球范围内搭建 EPCglobal 网络具有重大的研究和现实意义。本论文对 EPCglobal 的体系架构进行一系列安全方面的研究，旨在增强该系统的安全性，促进其发展，为今后安全方面工作的开展提供思路和借鉴。本文所做的工作主要主要有：

（1）利用无证书公钥密码体制的优点，提出一种基于无证书的密钥协商协议，并证明其正确性与安全性。

（2)在分析了现有标签访问协议安全隐患的基础上提出一种符合 EPC C1G2（Class-1 Generation-2 UHF）标准的标签访问协议，并分析其有效性和安全性。

（3）分析 EPCglobal 体系架构中 ONS（对象名称解析服务）存在的安全隐患并提出采用 Tor（第二代洋葱路由）的防范对策，提出一种基于无证书的 Tor 协议。

（4）针对 EPCglobal 体系架构中 DNS 查询部分存在的安全漏洞，提出了一种基于无证书的安全 DNS 协议。

关键词 EPCglobal 无证书 安全 对象名称解析 EPC 信息服务

Abstract

There is neither the complicated problem of certificate management of traditional certificate-based public key cryptology, nor the problem of inherent key escrow of identity-based public key cryptology.

EPC (electronic product code) network is an advanced comprehensive system, of which the purpose is to set up a global open system for every single product in the world. The aim of EPCglobal is to promote and develop EPC network in all the industries in the world, to raise the transparency and the visibility of the information of trade unit in the supply chain by developing and managing the standard of the EPC network.

EPCglobal architecture has three security domains in practice, security domain consisting of tag and reader, security domain consisting of ONS query process and security domain consisting of DNS query process. Therefore, it is of big significance for promoting the construction of the EPC network in the whole world to take the advantage of the certificateless public key cryptology to enhance the security of EPCglobal system. This thesis researches the aspect of the security of the EPCglobal system, and the purpose is to enhance the security of the system. The main contents of this thesis are as follows:

1. Takes the advantage of the certificateless public key cryptology,and proposes a key agreement protocol based on the certificateless, and then proves its validity and security.

2. Analyses the present tag-reader secure communication protocol, and proposes a tag-reader secure communication protocol conforming the EPC C1G2(Class-1 Generation-2 UHF) standard.

3. Analyses the potential security risks in the ONS (Object Naming Service) of the EPCglobal architecture, and proposes a Tor (The Second Generation Onion Router) protocol based on certificateless.

4. Analyses the security risks in the DNS query part of the EPCglobal architecture, and proposes a kind of DNSSEC (Domain Name System Security Extensions) protocol based on certificateless.

Key Words: EPCglobal; certificateless; security; ONS; EPCIS

目 录

Table of Contents

第一章 绪论

20 世纪 70 年代开始在全球推广应用的以商品条码为核心的 EAN•UCC 系统（全球统一标识系统）现在已经深入到日常生活的每个角落，在通信技术、互联网技术、射频识别技术等新技术的推动下，一种能够保证供应链上各个环节信息的自动、实时识别的全新网络构架——“EPC 网络”正日渐清晰起来[1]。

1.1 课题研究背景和意义

在不久的某一天，你在超市里挑好物品后再需要排队等候结账，直接走出商店就行了；你驾驶着车到某处游玩路过收费站时直接驾车过去即可，路费将自动从你的卡上扣除；你回家后冰箱的液晶屏幕提示你前些日子买的牛奶快过期了，请尽快饮用；……上面的一切看起来是那么的方便快捷[2]，这主要得益于上个世纪末由麻省理工学院等大学提出的物联网项目，这个项目旨在解决世界上所有物体（甚至小到地上的一粒沙）的唯一识别。这些物体贴有其特定的标签设备，可被标签阅读器识别并连上互联网，从而便构成了一个可以覆盖全球任意地点包含任何物品的网络——“EPC 网络”[3]。

“EPC 网络”的关键是“电子产品代码”（Electronic Product Code，EPC），即是贴在物品上的标签中含有的那一串数字字符。标签设备存储了这些电子产品代码数据，利用阅读器可以将其读出并送至 EPC 网络，网络中的数据库存储了与该 EPC 相关联的物品的所有信息，如产品的生产地点、发货目的地、发货日期、有效日期等等。随着产品的转移或变化，这些数据也会进行实时更新[4]。人们在全球的任意地点都可以通过互联网查询了解相关物品的实时信息。

RFID（射频识别）是一种非接触式的自动识别技术，它通过射频信号自动识别目标对象并获取数据，识别工作无须人工干预，并可工作于各种恶劣环境。目前，国际上 RFID 技术发展迅速并且已经在很多国际大公司中进入实用阶段，采用 RFID 最大的好处是可以对企业的供应链进行高效管理以有效地降低成本[5]。但是由于每个 RFID 标签中都有一个惟一的识别码（ID），如果它的数据格式有很多种且互不兼容，那么使用不同标准的 RFID 产品就不能通用，这对全球

经济一体化的物品流通非常不利，标准不统一已成为制约 RFID 发展的重要因素之一。如何让这些标准互相兼容使得一个 RFID 产品能顺利地在世界范围中流通是当前急待解决的重要问题。

EPCglobal 是一个中立的非盈利性标准化组织，其前身是 1999 年 10 月在 MIT（美国麻省理工学院）成立的非盈利性组织 Auto-ID 中心。2003 年 11 月 1 日，EAN/UCC 正式接管了 EPC 在全球的推广工作，成立了 EPCglobal 负责管理和实施全球的 EPC 工作，同时，EPCglobal 将 Auto-ID 中心更名为 Auto-ID 实验室为 EPCglobal 提供技术支持[6]。EPCglobal 的主要职责是在全球范围内对各个行业建立和维护 EPC 网络，保证供应链上各环节信息的自动实时识别采用全球统一标准，EPCglobal 的成立为 EPC 系统在全球的推广提供了强有力的组织保障，它通过搭建一个可以自动识别任何地方、任何事物的开放性全球网络（即 EPC 网络），为公司提供某些他们梦寐以求的、几乎完美的供应链可见度[7]。

但是 EPCglobal 标准构成的 EPC 网络体系架构（以下简称 EPCglobal 体系架构）在实际应用中存在三大安全区域：标签与阅读器构成的安全区域、ONS（对象名字服务）查询过程的安全域、DNS 查询过程的安全域。在标签和阅读器构成的安全域中，首先由于标签本身存在的一些局限性，如：计算能力有限、存储空间有限等，使得设计安全的密码机制受到诸多的限制。另外由于标签与阅读器之间的数据通信链路是无线通信链路，无线传输的信号是开放的，这给非法用户侦听带来了方便。因此，设计安全、高效、低成本的标签安全通信协议成为一个新的具有挑战性的问题[8]。另外在 ONS 查询过程的安全域中，由于 ONS 查询过程中本地服务器是以明文的方式发送对 EPC 的查询信息，攻击者非常容易就可以窃听到本地服务器的查询内容，进而推出标签的 EPC 信息，造成标签 EPC 信息泄露，解决这种私密信息泄露问题成为了当前研究的热点[9]。而在 DNS 查询域中，由于 EPCglobal 系统的 ONS 查询部分是建立在 DNS 查询之上，而 DNS 在设计之初并没考虑其安全问题，它既没有在内部对其交互的数据进行认证和安全性检查，也没有对 DNS 服务进行访问控制等方面的限制，结果造成了诸多安全漏洞。为了解决 DNS 查询存在的安全问题，各种安全方案被提出来，其中以 RFC2535DNS 安全扩展协议影响最大[10]。