View metadata, citation and similar papers at core.ac.uk
brought to you by CORE
provided by Xiamen University Institutional Repository

学校编码：10384　　分类号_____密级_____
学号：17720071150715　　UDC_____

厦门大学

硕 士 学 位 论 文

EPC 网络的自动信任协商机制研究

Study on Automated Trust Negotiation Mechanism in EPC Network

郝秀荣

指导教师姓名：韩水华 教授
专 业 名 称：管理科学与工程
论文提交日期：2010 年 4 月
论文答辩时间：2010 年 月
学位授予日期：2010 年 月

答辩委员会主席：_____
评 阅 人：_____

2010 年 04 月

厦门大学博硕士论文摘要库

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

厦门大学博硕士论文摘要库

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　　日

厦门大学博硕士论文摘要库

厦门大学博硕士论文摘要库

摘 要

无线射频识别（Radio Frequency Identification，RFID）结合其他通讯技术，可以即时地提供贴有 RIFD 标签产品的信息，利用这些信息可以追踪产品在整个供应链中运动的情况，从而提高了供应链的可视性，使供应链的管理更加高效。但要实现这些好处，供应链企业必须共享这些信息，同时供应链企业还需要知道在哪里可以找到这些信息。

EPCglobal 标准组织提出了发现服务（Discovery Services，DS）来解决该问题，可以把发现服务看作是电子产品代码网络（Electronic Product Code Network，EPC 网络）的一个受限的搜索引擎。授权用户能够使用 EPC 码向发现服务提出查询请求，发现服务则向用户返回拥有与该 EPC 码相关信息的 EPC 信息服务（Electronic Product Code Information Service，EPCIS）的链接地址，然后，请求者可以直接通过这些链接来得到更详细的信息。

EPC 网络的发现服务框架的不足是：只能查找已知的供应链参与者所持有的 EPC 信息资源，而无法定位到未知的供应链参与者，因此，无法真正实现信息共享与协同工作。为使同一供应链上的企业之间建立信任关系，就需要解决企业之间的资源授权与访问控制问题。本文拟提出自动信任协商（Automated Trust Negotiation，ATN）的方法，来解决这一问题，从而使企业在保护企业信息隐私的前提下，与未知供应链参与者之间共享 EPC 信息。

论文首先介绍 EPC 网络及自动信任协商的研究现状。接着对 EPC 网络的发现服务的工作流程进行了详细的介绍，指出其中存在的不足，并把自动信任协商机制引入到 EPC 网络体系中。然后，通过对现有的主要的几种信任协商系统的比较，选择一种适合 EPC 网络应用的信任协商系统 TrustBuilder2。最后，针对具体的供应链应用场景，我们制定访问控制策略与数字证书，并在 TrustBuilder2 系统的基础上进行信任协商的实现，说明自动信任协商可以对 EPC 网络现有的访问控制机制进行补充。

关键字：EPC 网络；自动信任协商；访问控制策略

厦门大学博硕士论文摘要库

厦门大学博硕士论文摘要库

Abstract

To improve the visibility of supply chain and make the supply chain management more effectively, combined with other communication technologies, RFID is used to track the movement of products attached with RFID tags in supply chain and provide products details. To realize these advantage, supply chain participants should share products information and the partners need to know where to find these information.

To solve this problem, EPCglobal consortium promoted Discovery Services architectures. EPC global can be treated as a limited search engine of EPC network. Authorized users can ask for a query requirement by using EPC code. Discovery Services sends back the related EPCIS addresses. Then, the user may directly obtain more detailed information through these links.

Discovery service architectures is limited to identify participants already known，fails to locate unknown participants. Therefore, information sharing and cooperation are just slogan. In order to establish trust between supply chain partners，authorization and the access control must be considered. Then, an Automated Trust Negotiation is proposed to solve this problem.

Firstly, this thesis reviewed related literatures on EPC network and Automated Trust Negotiation (ATN) and introduce workflow of Discover Service in EPC network. Defects of Discover Service are specially studied and ATN is introduced to solve this problem. Secondly, several trust negotiation systems are studied and try to find out the best –matched system to EPC Network. Then, several cases about ATN application are studied. Based on TrustBuilder2 system, access control policies and credentials are defined to test ATN application. Finally, conclusion suggests that ATN improves the information sharing in EPC network.

Key words: EPC Network; Automated Trust Negotiation; Access Control Policy

厦门大学博硕士论文摘要库

厦门大学博硕士论文摘要库

目 录

厦门大学博硕士论文摘要库

厦门大学博硕士论文摘要库

Contents

厦门大学博硕士论文摘要库

厦门大学博硕士论文摘要库

第一章 绪论

1.1 问题的提出

为了应对与供应链相关的成本压力，企业使用了很多方法来提高需求、销售预估及库存等信息的准确性。然而，可以用来解决这些问题的一些信息却在其他供应链企业手中。而且，为了有效的匹配供需，供应链上的企业之间需要进行紧密的合作。

EPC 网络允许公司通过追踪产品在整个供应链的情况，可以使业务流程更加高效，能更好地满足客户的需要。但要实现这些好处，企业需要共享一些信息和合作伙伴公司需要知道在哪里可以找到它。

EPCglobal 组织提出了发现服务（DS）来解决该问题。可以把发现服务（DS）看作是 EPC 网络的一个受限的搜索引擎。授权用户能够用唯一的 EPC 码查询发现服务来获取指向 EPC 信息服务（EPCIS）的链接地址，然后通过这些链接地址可以查询更详细的 EPC 信息。

EPC 网络系统提出的发现服务框架的不足是：只能查找已知供应链参与者所持有的 EPC 信息资源，而无法定位到未知的供应链参与者，因此，无法真正实现信息的共享与协同工作。为使同一供应链上的企业之间建立信任关系，就需要解决企业之间的资源授权与访问控制。本文拟提出自动信任协商（Automated Trust Negotiation，ATN）机制来解决该问题，从而，促进 EPC 信息在供应链企业之间的共享，提高供应链的透明化程度。

1.2 EPC 网络访问控制的研究现状

为了解决供应链上的 EPC 信息共享问题，EPCglobal[15]组织提出的 EPC 网络结构，其中的核心组件，包括 EPCIS、域名解析服务（ONS）和 EPCIS 发现服务。EPCglobal 现有的提案中规定在 EPCIS 的查询接口必须提供 EPCIS 和用户之间的双向认证方式，该认证将决定授权和执行访问控制。EPCglobal 没有详细介绍这些认证如何执行，以及安全策略如何构建。

厦门大学博硕士论文摘要库

BRIDGE[①]小组的 BT Research 等[1]总结了已有的 RFID 安全技术，提出了基于 RFID 设施的开放的、合作的业务应用应该考虑的安全需求。指出如果不对 EPCIS 的访问控制策略制定方法进行标准化，每个公司采用不同的安全策略结构，策略的不一致性可能会导致安全漏洞。该文建议用 XACML[②]制定 EPCIS 的访问控制策略。针对不同的访问者，用 XACML 制定的访问控制策略会给出同意、拒绝或不适用等评测结果值，但没有进行进一步协商的机制。

Eberhard Grummt[2]研究了 EPC 网络的多方合作的特性，及该特性对访问控制的影响。提出了实现 EPCIS 和发现服务的需求和建议方法。文中提到为了支持物品在整个供应链的追踪，EPCIS 可能会被陌生的公司查询。如：零售商 C 想要了解 p 产品的物流线路信息，就需要查询制造商 A 的 EPCIS。但是，零售商 C 从分销商 B 处购买 p 产品，制造商 A 可能很难确定零售商 C 的访问请求是否合法。因此，提出用权限的委托的方法可以来解决该问题。文中指出 EPC 网络没有充分的强调安全性，设计的发现服务处于核心位置，意味着所有的人都必须信任该发现服务提供者，这使发现服务易受攻击。

SAP 公司的 RFID 研究专家 Chris Kürschner 等[3]针对 EPCglobal 提出的发现服务框架的不足：只能查找已知供应链参与者所持有的 EPC 信息资源，而无法定位到未知的参与者。为了使陌生的供应链参与者可以共享信息，该文提出了自动合同协商(Automated Contract Negotiation)和费用补偿(Billing Pay-per-information)两个机制，如图 1-1 所示，但未对此做深入的讨论。

杜超坎[4]针对 EPC 网络可能存在的安全隐私风险，从策略管理的层面，提出一个适合 RFID 网络部署的访问控制框架体系。在 EPC 网络的隐私保护需求的基础上，分析讨论了 EPC 网络发现服务各种类型的访问控制策略，并采用合并决策算法解决信息发布者和发现服务提供者访问控制冲突问题。

总体来说，对 EPC 网络访问控制的研究文献还是比较少。EPC 网络的相关标准也逐步完善中。

① BRIDGE[21]（Building Radio Frequency Identification for the Global Environment）是一个 RFID 研究项目，该项目由欧盟资助，全球多个科研机构、标准组织（如 GS1 国际物品编码协会）和大学，包括中国的复旦大学都参与了这个项目，项目的目的是解决实施 RFID 的各种障碍和问题。

② 可扩展的访问控制标记语言（eXtensible Access Control Markup Language，XACML）是一种基于 XML 的适用于描述分布式系统访问控制的语言，它既是一种访问控制策略语言，也是一种请求（Request)/响应（Response)描述语言。

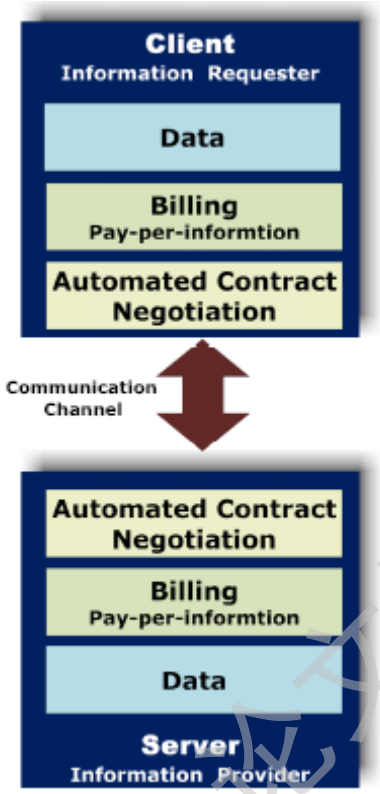

图 1-1：在 EPCIS 中增加自动合同协商和费用补偿机制

资料来源：Chris Kürschner．discovery service design in the EPCglobal network towards full supp chain visibility[3]，2008

1.3 自动信任协商研究现状

1.3.1 自动信任协商的提出

1996年，M.Blaze等人[5]首先提出信任管理（Trust Management，TM）的概念，为解决分布式环境中新应用形式的安全问题提供了新思路。信任管理的基本思想是承认开放系统中安全信息的不完整性，系统的安全决策需依赖可信第三方提供的附加安全信息。信任管理的内容包括：制定安全策略、获取安全数字证书、判断安全信任征集是否满足相关的安全策略等。信任管理要回答的问题可以表述为“安全数字证书集C是否能够证明请求r满足本地策略集P”。

Winsborough等 [6]称这类信任管理系统为基于能力的授权系统，它们仍需要服务方预先为请求方颁发指定操作权限的数字证书，无法与陌生方建立动态的信任关系。依赖基于主体属性授权，是一种不同安全域之间的用户建立信任关系的

有效方法。

自动信任协商的定义是“通过数字证书、访问控制策略的交互暴露，使得资源的请求方和提供方自动地建立信任关系”[6]。迄今为止，自动信任协商的研究已得到迅速发展，提出了多种领先的研究方法和技术，但是，目前自动信任协商整体性研究工作尚处于初级阶段。

1.3.2 自动信任协商模型概述

图1-2说明了自动信任协商的通用体系结构。协商的参与者们都拥有一个安全代理，通过这个代理完成双方的协商过程。资源请求者通过安全代理向提供者发送请求服务，发起一次协商过程。根据访问控制策略，安全代理来决定哪些本地受保护的资源，例如服务、数字证书和策略可以暴露给对方。访问控制策略描述：请求者应该具有哪些属性，才能获得资源的访问权限。在自动信任协商系统中，协商者所拥有的属性是通过数字证书描述的。因此，访问控制策略实际上描述了请求者应该暴露哪些数字证书才能获得某个资源。

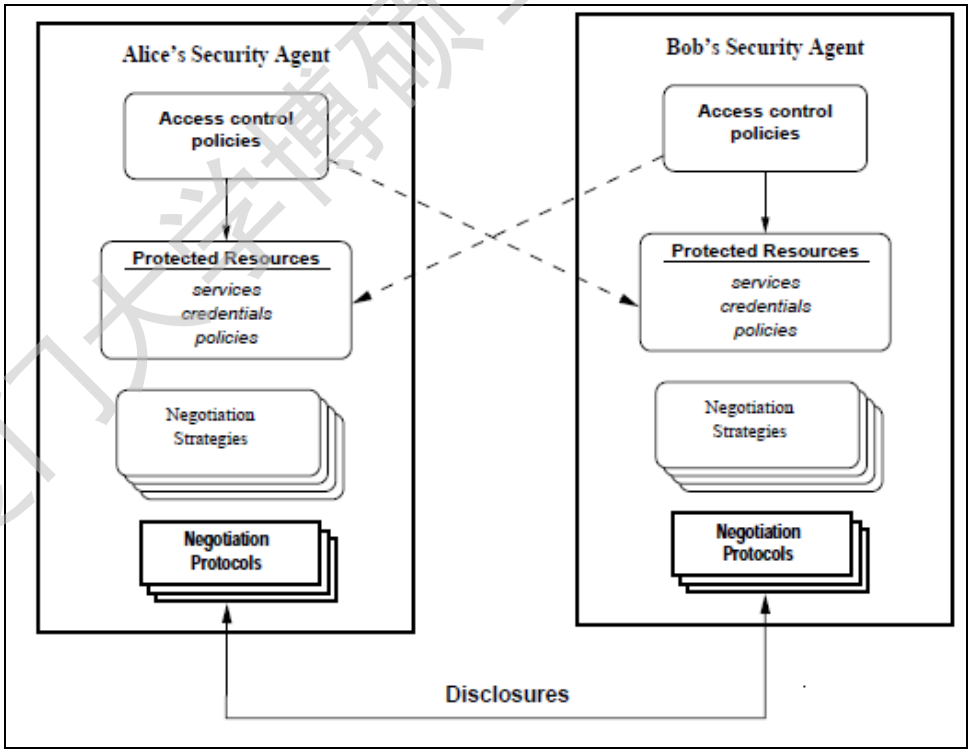

图 1-2：自动信任协商结构

资料来源：Yu T. Automated trust establishment in open systems[7],2003.

厦门大学博硕士论文摘要库

Degree papers are in the “Xiamen University Electronic Theses and Dissertations Database”. Full texts are available in the following ways:
1. If your library is a CALIS member libraries, please log on http://etd.calis.edu.cn/ and submit requests online, or consult the interlibrary loan department in your library.
2. For users of non-CALIS member libraries, please mail to etd@xmu.edu.cn for delivery details.

厦门大学博硕士论文摘要库