The Design and Implementation of Bluetooth Simple Pairing Based on NFC Technology

TangMin[1], Xiaonan[1], Chu En-Lai[2]

1. School of Information Engineering, Jingdezhen Ceramic Institute, Jingdezhen Jiangxi 333403, China

2. Department of Computer Science, School of Information Engineering, University of Science and Technology of Beijing, Beijing, 100083, China

1. tm902@sina.com，2. tttang888@163.com

Abstract: In order to improve the usability and security of Bluetooth pairing, Bluetooth Special Interest Group proposed a simple pairing strategy. Based on the simple pairing strategy and Bluetooth protocol, this paper provides a solution of simple pairing. It transmits parameters by NFC technology. Then this paper describes the particular hardware and software design of our solution. The results showed the feasibility and stability of this solution.

Keywords: Bluetooth; pairing; security; NFC

基于 NFC 技术的蓝牙简单配对设计与实现

唐敏[1]，肖楠[1]，楚恩来[2]

1. 景德镇陶瓷学院信息工程学院，景德镇，中国，333043

2. 北京科技大学，北京，中国，100083

1. tm902@sina.com，2. tttang888@163.com

【摘要】为了提高蓝牙配对策略的安全性和易用性，蓝牙特别兴趣小组提出了简单配对的策略。本文基于简单配对策略和蓝牙协议体系结构，并结合系统硬件及软件体系结构特点，提出了一种实现简单配对的应用方案。通过 NFC 技术传输配对参数来完成简单配对。文中给出了该方案详细的硬件设计和软件设计。测试结果显示了此方案的可行性和稳定性。

【关键词】蓝牙；配对；安全；近距离无线通信

1 引言

蓝牙（Bluetooth）是一种新型的低成本、低功率、近距离无线连接技术，实现数据与语音的无线传输。蓝牙设备的工作频段选在全球通用的 2.4 GHz 的 ISM（工业、科学、医学）频段。蓝牙技术已获得了全球认可，它是当今市场上支持范围最广泛，功能最丰富且安全的无线标准。与其他无线通信技术一样，由于采用开放的信道作为通信介质，因此蓝牙技术在安全性方面也面临各种威胁，例如假冒、窃听、非授权访问和服务拒绝。

蓝牙安全系统依赖于长度为 8—128 比特的用户个人身份识别码（Personal Identification Number，PIN）。为了建立安全的蓝牙通信链路，在双方设备首次建立连接时或是通信的链路密钥丢失时，需要双方设备提供相同的 PIN 码，完成设备间的认证，这个过程叫做配对。为了简化配对步骤提高蓝牙通信的安全性，蓝牙特别兴趣小组（Bluetooth Special Interest Group，SIG）在蓝牙规范 v2.1 中提出了简单配对支持利用蓝牙带外传输完成配对。

我们使用近距离无线通信技术(Near Field Communication， NFC)，作为蓝牙带外传输机制，实现了简单配对的整套方案。NFC 设备和蓝牙设备工作频率互不干扰，使其能与蓝牙在同一个产品中共存，它的作用距离 10 厘米左右，从而排除了第三方进行的中间人攻击。Frost & Sullivan 估计，未来 3 到 5 年将有 1/3 的手机具备 NFC 功能，Strategy Analytics 预测，至 2011 年全球基于移动电话的非接触式支付额将超过 360 亿美元，可见本文研究的研究工作具有广阔的应用前景。

2 核心技术

在我们的设计和实现方案中使用的核心技术包括蓝牙技术和 NFC 技术。

2.1 蓝牙技术

蓝牙协议体系结构可分为底层硬件模块、中间协议层和上层应用层三大部分。链路管理层（Link Manager Protocol）、基带层（Base Band）和蓝牙无线电信道构成蓝牙的底层模块。基带层负责跳频和蓝牙

数据及信息帧的传输。链路管理层负责连接的建立和拆除以及链路的安全和控制，它们为上层软件模块提供了不同的访问入口，但是两个模块接口之间的消息和数据传递必须通过蓝牙主机控制器（Host Controller Interface，HCI）接口的解释才能进行。HCI 是软硬件之间的接口，它提供一个调用下层 BB、LMP 状态和控制寄存器等硬件的统一命令接口。HCI 以上的协议软件实体运行在主机上（我们的解决方案中，这部分运行在 PC 上），而 HCI 以下的功能由蓝牙设备来完成，二者之间通过对两端透明的 HCI 传输层进行交互。

中间协议层包括逻辑链路控制与适配协议（Logical Link Control and Application Protocol）、服务发现协议（Service Discovery Protocol）、串口仿真协议（RFCOMM）和电话控制协议规范（Telephone Control Protocol）。逻辑链路控制与适配协议完成数据拆装、服务质量控制、协议复用和组提取等功能，是其他上层协议实现的基础，因此也是蓝牙协议栈的核心部分。服务发现协议为上层应用程序提供一种机制来发现网络中可用的服务及其特性。串口仿真协议作为一个电缆替代协议，它通过在蓝牙的基带上仿真 RS232 的功能，为高级业务提供传输能力。

在蓝牙协议栈的最上部是各种高层应用框架（Profiles）。其中较典型的有拨号网络（Dial-up Networking）、耳机（Headset）、文件传输（File Transfer）等，分别对应一种应用模式。所有这些应用使用的安全链接都是从配对开始的，加密通信的安全性依赖与配对过程产生的通信密钥。由此可以看出配对在蓝牙安全体系中的重要地位。

2.2 NFC 技术

NFC 技术是由飞利浦公司发起，由诺基亚、索尼等著名厂商联合主推的一项无线技术。NFC 由非接触式射频识别（RFID）及互联互通技术整合演变而来，在单一芯片上结合感应式读卡器、感应式卡片和点对点的功能，能在短距离内与兼容设备进行识别和数据交换。NFC 技术主要基于 13.56MHz 频率运行的射频技术，典型操作距离只有几厘米，数据传输速度可以选择 106kbit/s，212kbit/s 或 424kbit/s，将来可提高至 1Mbit/s 左右。NFC 技术在 ISO 18092、ECMA 340 和 ETSI TS 102 190 框架下推动标准化，同时也兼容应用广泛的 ISO 14443 Type-A、B 以及 FeliCa 标准非接触式智能卡的基础架构。

NFC 协议中使用到两个角色：Initiator（发起方）与 Target（目标方），Initiator 指最先发起沟通与发送无线电波的一方（自身有电源供给），负责发起连接和控制数据交换。Target 则为回应的一方，Target 若是依赖载波电能的吸收而运作属于被动运行模式，若自身有电源供给则属于主动运行模式。在主动模式下，每台设备要向另一台设备发送数据时，通讯双方都要产生自己的射频场，以便进行通信。在被动模式下，启动 NFC 通信的设备，Initiator 在整个通信过程中提供射频场，负责发起连接和控制数据交换。它可以选择 106kbps、212kbps 或 424kbps 其中一种传输速度，将数据发送到 Target 设备。Target 不必产生射频场，而使用负载调制技术，即可以相同的速度将数据传回 Initiator。

NFC 技术支持三种不同的操作模式：①读写模式（对 FeliCa 或 ISO 14443A 卡的读写）主动模式下，NFC 终端作为一个读卡器，主动发出自己的射频场去识别和读/写别的 NFC 设备。②卡模式（如 FeliCa 和 I S O 14443A / MIFARE 卡的通信），被动模式下，NFC 终端可以模拟成一个卡被读/写，它只在其他设备发出的射频场中被动响应。③N F C 模式（NFC 芯片间的通信），在该应用模式中，NFC 设备之间建立点对点的通信，在近距离内进行数据的交换。

3 简单配对过程和原理

传统蓝牙配对策略面临的安全挑战主要包括被动监听和主动控制两大类。被动监听是指第三方设备监测两个蓝牙设备之间的通信，通过逆向过程推导出双方使用的链路密钥，如：利用监听的 PIN 码攻击。主动控制是指第三方设备直接充当信息的中转站，控制两个蓝牙设备的通信，如：中间人攻击（Man-in-the-Middle，MITM）。这些威胁阻碍了蓝牙技术的应用和推广，在这样的背景下，蓝牙特别兴趣小组经过多年研究，提出了简单配对的策略来降低蓝牙设备在配对过程中受到攻击的可能性，从而提高蓝牙通信的安全性。

简单配对改进了链路密钥创建的算法以及两个蓝牙设备 LMP 之间安全信息交互的方式。密钥创建方式采用基于椭圆曲线的 Diffe-Hellman 密钥交换协议，每个设备生产一个公私钥对。通过 FIPS P-192 曲线函数利用私钥和对方公钥计算各自的 DHkey 值（如果信息正确，计算出的这两个值相等），并通过 SHA-256x 计算认证使用的 Hash 值 C_Value，将各自设备的蓝牙地址，C_Value，随机数 R_Value 通过蓝牙带外传输机制传递给对方设备。双方设备利用接收到的值计算对方设备的 C_Value 来和接受收到的 C_Value 作对比，进行第一次认证，这次认证成功后双方使用通过蓝牙信道传递来的对方设备新的随机数值和自己的 DHkey 值，再利用 SHA-256 算法计算第二次认证使用的确认值，并通过蓝牙信道传递给对方。两次认证成功后，双方设备分别计算进行加密通信使用的密钥，简单配对完成。

简单配对由于使用了基于椭圆曲线的 Diffe-Hellman（ECDH）密钥交换机制，使得简单配

978-1-935068-01-3 © 2009 SciRes.

对能够防止强度较大的被动偷听攻击，但是它不能防止 MITM 攻击。这就要依靠蓝牙带外传输机制来防止 MITM 的攻击方式。

4 系统实现方案

4.1 系统设计

本系统所完成的功能是：控制配对过程，利用 NFC 设备传递配对参数，来完成蓝牙简单配对。系统有多个模块组成，每一个模块是一个独立的运行单元，完成特定的功能。整个系统分为 PC 端控制模块和蓝牙模块及 NFC 模块三个部分。蓝牙模块包括蓝牙硬件和蓝牙设备控制软件。NFC 模块包括 NFC 硬件设备和 NFC 控制软件。系统的运行由 PC 端应用层程序控制，整体结构如图 1 所示。

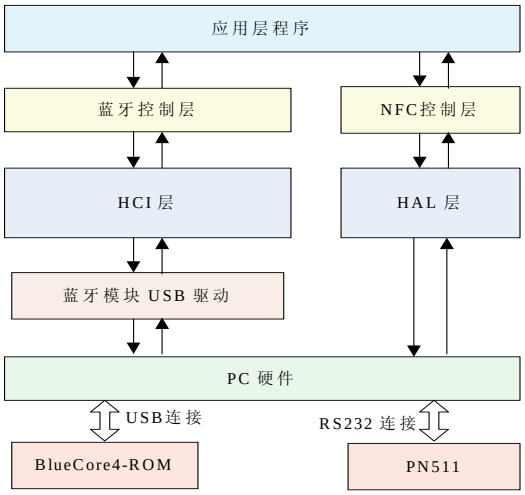

图 1：系统总体结构图

4.2 硬件设计

本系统是基于 PC 来开发的，硬件部分主要包括蓝牙硬件模块，NFC 硬件模块。蓝牙硬件通过 USB 与 PC 连接，NFC 设备通过 RS232 与 PC 连接。

目前常用的蓝牙芯片方案有多芯片方案（RF 芯片、基带芯片和微处理器芯片）、双芯片方案（RF 芯片和含 CPU、RAM 和 Flash 的基带芯片）、单芯片方案（将 RF、基带和 CPU、RAM 及 Flash 集成在一片 CM0S 芯片上）。本文采用单芯片方案，选用 CSR 公司提供的 BlueCore4-ROM 芯片，该芯片是一款针对语音和数据通信的单芯片无线电和基带蓝牙系统，其系统结构如图 2 所示。它非常省电，需要很少的外部元件，支持 CSP 和 VFBGA 封装，支持蓝牙 v2.1+EDR 标准，传输速率最高达 3Mbps，支持 Piconet （微型网）和 Scatternet （散射网），同时能够处理扩展的 SCO （eSCO）编码。BlueCore4-ROM 同样向后兼容 v1.1 或 v1.2 设备。支持 USB、UART、PCM 等接口，用于无线耳机、PDA、数字相机和鼠标、键盘等数据收发终端的嵌入式系统设计。

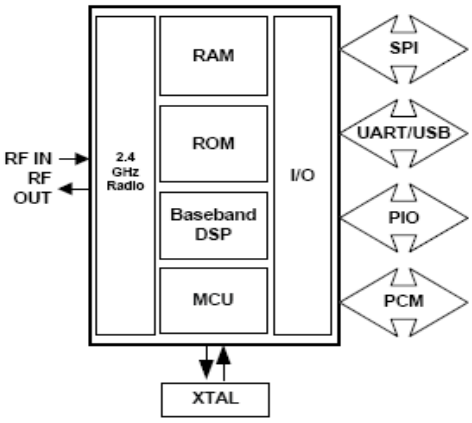

图 2: BlueCore4-ROM 系统结构框图

BlueCore4-ROM 通过透明传输层 HCI 与 PC 进行通信。PC 端和 BlueCore4-ROM 中都有 HCI，它们具有相同的接口标准。BlueCore4-ROM 中的 HCI 解释来自 PC 的信息并将信息发向相应的硬件模块单元，同时还将模块中的信息（包括数据和硬件/固件信息）根据需要向上转发给 PC。PC 与 BlueCore4-ROM 通过指令—应答（Command-Response）方式实现控制，主机（PC）向主机控制器（蓝牙芯片）发送指令分组。主机控制器执行指令后，通常会返回给主机一个指令完成事件分组，该分组携带有指令完成信息。对于有些分组，不返回指令完成事件分组，但返回指令状态事件分组，用以说明主机发出的指令已经被主机控制器接收并开始处理。如果指令执行出错，返回的指令状态事件分组就会指示相应的错误代码。

采用 NXP 公司的 PN511 作为 NFC 芯片，它是一款用于 13.56MHz 非接触通信的高集成度收发器 IC。这个收发器 IC 利用先进的调制和解调技术，完全集成了 13.56MHz 下的各种主动/被动式非接触通信方法和协议。PN511 模块支持 3 种不同的操作模式。

我们采用的是 NFCIP-1 标准的被动通信模式，工作图如图 3 所示。传输速率使用 NFCIP-1 标准所定义的 106 kbit/s（ISO 14443A 标准），选取这个最慢速度的原因是由于我们所需要传输的数据量较小。主设备产生 13.56MHz 的射频场并发起 NFCIP-1 通信，目标设备采用负载调制的方式对主设备命令进行应答。

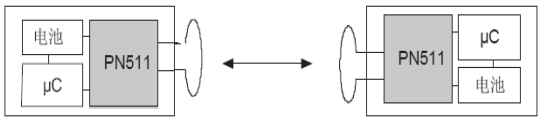

图 3：NFC 应用模式场景图

4.3 软件设计

系统的软件在设计过程中采用分层，多模块来实现的。整个软件以事件为触发，以消息机制为基础，各个模块（或任务）之间以消息进行通信。整个软件系统主要由蓝牙设备控制软件层，NFC 控制软件层，应用层程序组成。蓝牙设备控制软件包括 HCI 模块（完成向蓝牙硬件收发 HCI 命令的功能），蓝牙控制模块（控制蓝牙硬件和维护蓝牙通信的整个过程、状态）。NFC 控制软件包括 HAL 模块（NXP 公司提供的能够控制 PN511 芯片的硬件抽象层 API），NFC 控制模块（完成需要的 NFC 设备操作和设备间的通信）。应用层程序模块：全局控制整个程序的运行，与用户交互，处理每个模块间的通信。

PC 端软件部分与蓝牙硬件基于 HCI 接口进行通信。在协议的实现上与一般协议之间的通信概念和机制相同。层内通信依据本层的协议规定进行交互。层间通信使用请求、确认、指示、响应四种原语实现。层内与层间通信依据信道状态机进行协调。整个系统软件运行流程如图 4 所示。

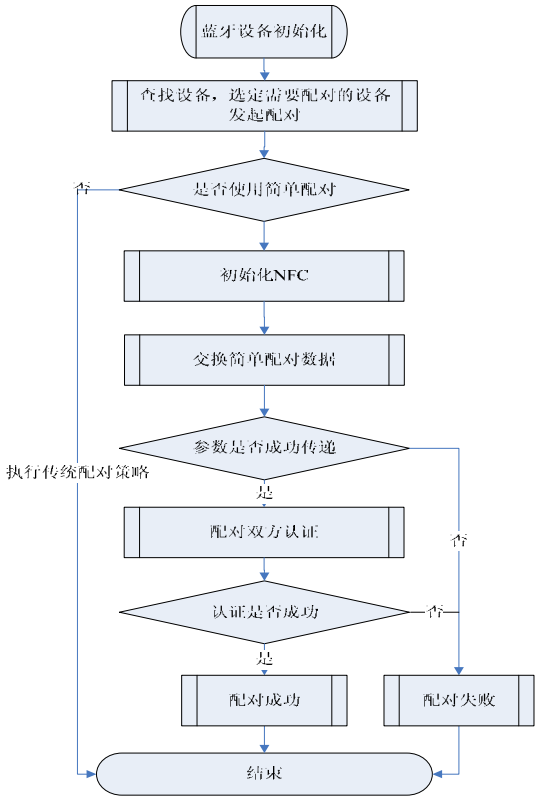

图 4：软件流程图

首先是蓝牙软件部分，整个过程由应用层程序触发，它调用蓝牙控制模块接口，蓝牙控制模块通过调用 HCI 模块，向蓝牙硬件发送 HCI 命令，并接受命令执行结果等信息。配对申请者初始化本地蓝牙设备，将其设置成支持 NFC 的简单配对模式。通过查找，找到需要与其配对的设备，发起配对。当配对验证者收到申请者的配对请求时，同时接收到一个 HCI 事件 IO_Capability_Request，要求提供是否支持 NFC 简单配对。应用层程序利用回调函数（在应用层程序中实现一个回调函数，将这个回调函数注册到蓝牙控制模块中）提供自己是否支持 NFC 简单配对，在蓝牙控制模块执行 HCI 命令 HCI_IO_Capability_Response，并带有一个参数告诉配对申请者自己是否支持 NFC 的简单配对。如果配对如果配对申请者收到对方设备支持 NFC 简单配对，继续下面简单配对过程，否则执行传统配对方式。在配对验证设备返回支持 NFC 简单配对的同时，执行 HCI_Read_OOB_Data 命令，通知蓝牙硬件计算本地的简单配对的两个重要 Hash 值 C_Value 和 R_Value，执行完这条命令后，会返回给上层应用程序两个 16 字节的值 C_Value 和 R_Value。再执行命令 HCI_Read_BD_ADDR 获得本地蓝牙设备的 6 个字节的地址 BD_ADDR。将这三个值由应用层程序传给 NFC 控制模块，存储在 NFC 设备的 ROM 中。当配对申请设备收到对方设备支持 NFC 简单配对的消息时，也执行 HCI_Read_OOB_Data 命令和 HCI_Read_BD_ADDR 命令获得本地设备的这三个值存储在与它相连的 NFC 设备的 ROM 中。当两方的 NFC 设备都存储了简单配对的三个参数后，由 NFC 控制模块通知应用程序数据准备好。这时两个设备会收到 HCI 事件 Remote_OOB_Data_Request，应用层程序会在界面上提示用户将两个 NFC 设备靠近来完成简单配对。这三个参数通过 NFC 技术传递远端设备。收到这些数据后，双方设备执行命令 HCI_Remote_OOB_Data_Request_Reply，参数为从 NFC 芯片中获得的对方数据，将数据传送给蓝牙芯片。由蓝牙芯片检查收到的 C_Value 值，与自己计算出来的对方设备的 Hash 值是否一致。在一致的情况下蓝牙芯片利用蓝牙链路传来的对方设备的随机数和自己生成 DHkey 计算第二次认证需要的验证码，第二次认证成功后，双方生成通信使用的链路密钥，简单配对完成。

为了节省功耗本文中采用发起配对后再初始化 NFC 设备的方式。由于初始化 NFC 设备需要一定的时间（大约需要一秒钟），这样对配对时间会有一定的影响，但是与减少功耗来比是值得的。使用 NFC 设备的被动通信模式，应用模式采用点对点的通讯模式。由于 NFC 设备在通信时需要区分 Initiator 和 Target。在本文的设计中将分别实现 Initiator 和 Target 端。我们采取的策略是配对申请者为 Target，验证者为 Initiator，主要过程如下：

1. 本地NFC硬件设备初始化，包括以下几个过程：

a) 调用函数phHalNfc_Enumerate( )，初始化相关硬件参数，显示与PC连接的周边NFC设备。

978-1-935068-01-3 © 2009 SciRes.

b) 选择一个NFC设备，利用函数 phHalNfc_Open( ) 建立PC与NFC设备的通路。

c) NFC控制程序通过phHalNfc GetDeviceCapabilities( ) 获得硬件性能参数，供后面的功能使用。

2. Initiator 和Target的初始化，在这里分开来处理：

a) Target模式设备

i. 通过函数phHalNfc_StartTargetMode( )，设置本地设备进入Target模式，等待Initiator设备轮询。

b) Initiator模式设备

i. 将本地的NFC设备设置为 Initiator，同时调用函数phHalNfc_Poll( )搜寻在自己射频场中的Target设备。

ii. 选定检测到的Target设备，设置传输速率为106kbit/s，利用函数phHalNfc_Connect( )与其建立点对点的连接。

3. Initiator与Target之间数据的传输：

a) Initiator 设备利用函数phHalNfc_Transceive( ) 将配对数据BD_ADDR，C_Value,R_Value发送数据给Target，并等待Target的给出的相应，或是超时发生函数返回。

b) Target设备利用函数phHalNfc_Receive( ) 接受 Initiator 发来的配对参数。

c) Target设备收到数据后，通过函数phHalNfc_Send( ) 将自己的配对数据发出应给Initiator。Initiator接收到Initiator的相应后，配对数据交换完成了，通信是半双工的。

4. 在传输数据完成后Initiator 利用函数phHalNfc_Disconnect( )主动断开与Target的连接，Target收到Initiator断开连接的信息会自动触发断开动作。

5. Initiator 和 Target 设备利用函数phHalNfc_Close( )关闭NFC设备与PC的连接，至此，NFC设备在一次简单配对中的任务就完成了。

5 测试结果

整个系统的开发和调试主要是在 PC 机上进行的。对设计和实现的简单配对方案，进行了测试。当看到“将 NFC 设备靠近来完成配对的提示后”，将两个 NFC 设备靠近，瞬间就完成了配对。测试结果见表 1。

表 1：简单配对测试结果统计表

测试距离（cm）	0—3	3—6	6—10	10 以上
配对成功率	大于 99%	99%	90%	小于 10%
配对完成时间（s）	小于 3	小于 3	小于 4	大于 5

从测试结果来看，与以前传统配对策略实现相比，在配对时间上大大减小。在传统配对策略应用模式下，假设用户输入 PIN 码为“0000”从发起配对到配对完成时间至少需要 10 秒，而我们实现的简单配对将配对时间缩短为 5 秒以下。随着距离增加，特别是在 6-10cm 时，配对的成功率下降，主要是由于 NFC 设备的工作距离决定的。此方案能够达到预期效果，设计和实现是合理的。

6 结束语

本文设计实现了一个基于NFC技术的蓝牙简单配对方案，与传统的配对方案相比，即提高了蓝牙配对过程的安全性，又改善了配对的易用性，并且极大地缩短了配对时间。经过测试表明方案是可行的。蓝牙芯片和 NFC 芯片将成为许多移动设备的标准配置，因此，我们的方案对推动蓝牙技术的应用和普及将有深远的意义，具有广阔的应用前景。

References（参考文献）

[1] Bluetooth Special Interest Group. Specification of the Bluetooth System. v.2.1. Core Specification. July 30, 2007. P1025-1040.

[2] Jin Chun, Lin Jinchao, Wan Baohong, Bluetooth protocol and source code analysis, National Defense Industry Press, 2006. P25-35, P110-132.金纯，林金朝，万宝红. 蓝牙协议及其源代码分析. 北京.国防工业 出版社.2006. P25-35, P110-132.

[3] Bluetooth Special Interest Group. Bluetooth Security White Paper. April 10. 2004. P35-38.

[4] Qian Zhihong, Yang fan, Zhou QiuZhan, Bluetooth technology development and application, Beijing University of Aeronautics and Astronautics Press, 2005. P45-50 钱志鸿，杨帆，周求湛. 蓝牙技术原理开发与应用. 北京.北京航空航天大学 出版社.2005. P45-50

[5] NFC Forum. “Near Field Communication White paper”, P6-7, http://www.ecma-international.org/activities/Communications/tc32-tg19-2005-012.pdf

[6] Ecma. ECMA - 352 , Near Field Communication Interface and Protocol (NFCIP - 2) [S] . GENEVA : EcmaInternational , 1st Edition/ December 2003. P10-11

[7] Ecma. ECMA - 340 , Near Field Communication Interface and Protocol (NFCIP - 1) [S] . GENEVA : EcmaInternational , 2nd Edition/ December 2004. P34-37

[8] BlueCore4-ROM WLCSP Product Data Sheet CS-101565-DSP 11 Dec 2007. P8-10.http://www.csrsupport.com/document.php?did=1932

[9] NXP Semiconductors PN511 Transmission Module ,Product short data sheet Rev. 3.1, 16 October 2006. P4-8