王晓华 编著

NFC技术进阶篇

- 移动支付技术的“战地手册”
- 雅观科技、恩智浦、小米、可为、紫光展锐、华米、麒麟、黑加手环等移动支付领域专家推荐

北京航空航天大学出版社
BEIHANG UNIVERSITY PRESS

NFC 技术进阶篇

王晓华　编著

北京航空航天大学出版社

内 容 简 介

本书主要介绍了NFC移动支付中的SE安全芯片，内容包括安全芯片安全等级的通用标准，安全芯片基本的硬件设计过程，OCR、CPLC、PUF、Glue Logic和Anti-tamper等硬件安全技术手段，安全芯片与外部主机端通信的详细GP & ISO/IEC7816-4软件接口等内容。

本书可作为NFC移动支付开发人员的参考用书。

图书在版编目(CIP)数据

NFC技术进阶篇 / 王晓华编著. -- 北京 : 北京航空航天大学出版社，2019.6

ISBN 978-7-5124-3022-8

Ⅰ. ①N… Ⅱ. ①王… Ⅲ. ①超短波传播－无线电技术 Ⅳ. ①TN014

中国版本图书馆CIP数据核字(2019)第117831号

NFC技术进阶篇

王晓华 编著

责任编辑 孙兴芳

*

北京航空航天大学出版社出版发行

北京市海淀区学院路37号(邮编100191) http://www.buaapress.com.cn

发行部电话：(010)82317024 传真：(010)82328026

读者信箱：emsbook@buaacm.com.cn 邮购电话：(010)82316936

涿州市新华印刷有限公司印装 各地书店经销

*

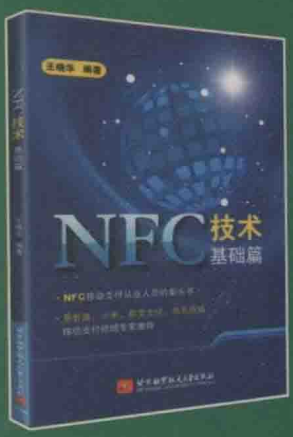
开本：710×1 000 1/16 印张：13.5 字数：241千字

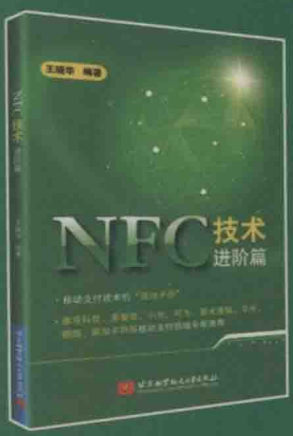
2019年6月第1版 2019年6月第1次印刷 印数：3 000册

ISBN 978-7-5124-3022-8 定价：49.00元

作者简介

王晓华　现就职于恩智浦(中国)管理有限公司，任高级程序经理职务，早年参与过PBOC移动支付相关标准的制定工作，最近的七年时间里主要工作于NFC移动支付相关领域，过去的主要工作经验集中在加密芯片软硬件设计、嵌入式软件应用和Android手机系统等方面，当前主要学习和关注的课题为IoT物联网安全和AI人工智能等。





策划编辑：胡晓柏
封面设计：runsign睿正设计 · 赫健

序 言

十月的北京开始进入初冬季节，天气慢慢变得干燥起来，我一直没有太适应这样的冬天。但是，对我而言，气温较低的月份却是一段让我有种心中窃喜的时期，因为它是使我能够静下心来思考一些问题的最佳时间。两年多前，北京航空航天大学出版社（简称北航出版社）出版了我人生中的第一本技术书——《NFC 技术基础篇》，现在回想起来还是非常的兴奋和感激。记得当初与胡老师沟通有关书中的细节时，对于如何做一套实用类的工具型案头入门书，双方观点竟然出奇的相似，我们都希望读者在阅读完全书后能够建立一个 NFC 的系统级概念，并能获得相关的技术，并且当读者在学习或者工作中再次遇到具体的 NFC 问题时，还能够对照《NFC 技术基础篇》这本书进行相关的研究；不希望把书做成偏实用的案例型的参考书，因为关于这方面的资讯，互联网上的资源异常丰富且更具时效性。

两年多来，通过从北航出版社的官方平台、线下书店、网络电商平台的用户评论、行业圈里的朋友和同事反馈等渠道了解到，大家还是非常认可《NFC 技术基础篇》这本书的！我认为这是一个作者最大的幸福。再次特别感谢胡老师的支持和认可，还有家人的理解以及对我无私的支持，当然还要感谢许多我认识的或未曾谋面的读者朋友。

我非常清楚地记得第一本书出版后读者的热烈反应，北航出版社也紧急催促我把 NFC 技术的进阶篇尽快完成并出版，我欣然答应了，但没有允诺具体的交稿日期，因为我确实无法预知我什么时候能交稿。自毕业参加工作以来，我工作时都有做学习笔记的习惯，笔记的主要内容就是学到的新知识和自己动手做实验的结果等。按照常理，书中最主要的资料都已经有了，编写书稿就是一个整理资料使其成册的过程，但是根据《NFC 技术基础篇》的出版经验，要完成一本书是需要花费大量的时间和精力的，学习笔记只是记录一个或者某个技术片段，离出版还有很大的距离，还需要做大量的工作。例如，对引用资料的来源和准确性要进行确认，对于实验或测试结果需要再次仿真，以确认是否准确和结果是否最优等。

去年六月份我对自己的职业生涯做了一个大的调整，把我的学习和研究方向从 NFC 和移动支付领域转到了 AI 人工智能和 IoT 物联网领域，所以这一年多来，我把工作和学习的重心放到了 AIoT 人工智能物联网的底层技术和通信协议的研究上，

对于着手准备《NFC 技术进阶篇》又耽误了一年半的时间。在对待自己感兴趣的新鲜事物时，自认为的优点是非常的好奇和乐观，缺点就是无法双线程进行学习，而且整体的学习进度是属于比较慢的那种，这个与我的阅读习惯非常相似。前几个月，有一次去朋友 Lorenzo 的家里玩，大家坐在一起交流《三体》的读后感，朋友提及他在四五个小时的飞行中就可以比较轻松地把类似《三体》这样的书的其中一部读完，而且他认为这是一种非常正常的阅读速度，但是这个速度却给了我不小的震撼。

因为去年工作重心转变的原因，自己又无法做到多线程工作，所以也就无法短期内安下心来准备《NFC 技术进阶篇》的相关资料。转眼又快到了年末，北京的冬天也来了，较低的气温让我的思维立马变得敏捷起来，是时候把两年多前欠下的东西还上了。前两个月和胡老师进行了一次电话沟通，告诉他我准备开始着手《NFC 技术进阶篇》书稿的事情，希望听取他的意见和建议，他的回复是他那边没有问题，我听完后倍感温暖。通过这几年与胡老师的沟通，从一开始对他的误解，主要是书稿出版时间的问题，致使我对他的工作方式和风格有些不解，再到后来我慢慢了解了他的工作性质，让我看到他身上谨慎的工作态度和专业精神，使我受益匪浅，他是我的良师益友！这一次，他一如既往地支持我撰写《NFC 技术进阶篇》一书，我就要更加认真地准备和规划，争取比上一本做得更好一些。

虽然这一年多以来我的研究方向转到了人工智能和物联网领域，其中，人工智能领域主要偏向深度学习，这与 NFC 以及移动支付所研究的范畴区别还是非常大的；但是物联网领域所使用的底层技术，特别是相关的连接技术，与 NFC 还是有很多相似之处的，本质上 NFC 也是物联网连接的一种技术。所以，通过这一年多对物联网的实际接触和探索，我发现 NFC 技术在物联网方面可应用的领域比移动支付还要大得多，例如，智能设备的耗材防伪、接入网络的快速配对连接和物联网设备鉴权等；而且现在就已有一些基于 NFC 技术的智能设备实现了相关应用，例如，小米空气净化器中主机端对滤芯配件的鉴权和防伪，SONY 相机支持 NTAG 快速进行手机连接配对等。

还有智能门锁这一年多来也发展迅速，虽然现在主流的智能门锁还是以生物识别为主，特别是指纹识别技术确实有其非常重要的安全和便捷属性，但是存量市场还是有许多非接触卡片的门禁市场，特别是对于 2B 企业端的客户，例如小区和单元入口等，目前物业运营商针对这种用户场景还是偏向推荐原来的物理卡片来做门禁市场。另外，就是现在的一些旗舰手机和穿戴设备也开始支持 NFC 技术，并且支持

复制传统门禁卡的 UID 到手机和穿戴设备上。基于上述原因，智能门锁市场中也开始有一些旗舰产品陆续支持 NFC 技术了。

我的一位同事，也是我非常尊重且极具创意精神的朋友——罗煜华先生，他是这个行业里的老兵了！我认为以他的工作资历和学习能力，完全没有必要再去看《NFC 技术基础篇》这类书了，但是，有一次我们刚好坐同一班飞机出差，他拿出《NFC 技术基础篇》那本书，非常认真地请教我一些具体的技术问题，然后在书本上认真地做着笔记，这着实让我非常的惊讶和感动！而且他还对这本书提出了一些改进意见和建议等，我也把这些内容记录到了我的手机便签中。其中，一个特别好的建议就是可以通过实际案例的形式，把相关的 NFC 和 SE 的技术穿插进去，这对于编写《NFC 技术进阶篇》一书是一个非常好的思路，我准备按照这个思路来编写这本书。在此特别感谢罗煜华先生！您是我见过的最优秀的市场销售人才之一，希望您永葆一颗创意的心。

另外，我想通过这本书来特别感谢曾经对我有过莫大帮助的两位领导——田陌晨先生和陈奕镇先生。田总能谋善断卓尔不群，极具商业洞察力和领导力；陈总温文尔雅宠辱不惊，对于商业见微知著且极具韧性。回想过去的八年，觉得自己非常幸运能在两位的领导下工作和学习，他们不仅带我走进了商业的世界，而且教会我许多为人处事的道理。田总教会我什么叫“人格平等，格局不同”，陈总则教会我“改变你能改变的，接受你不能改变的”，永远积极乐观地看待事情。在与两位领导的每次接触或者交谈中，总能学到一些东西或者激发我的一些思考；当我有新书出版，需要两位领导帮忙写推荐书评时，他们总是在第一时间给予反馈和支持，让我倍感温暖！在此，我衷心地祝愿两位领导在各自新的领域和岗位上，能够“长风破浪会有时，直挂云帆济沧海”。

我平时的工作非常忙，出差频率也非常高。我粗略地算了一下去年一整年的工作时段比例，近乎有三分之一的时间是在出差的途中，并且晚上还经常与国外的同事进行电话会议等，所以陪伴家人的时间非常少。而写书需要准备、整理相关资料，并将其论述成文，这需要花费更多的时间，因此留给家人的时间就更少了。但我的家人对我写书从未有过半句怨言，他们认为只要是我自己喜欢且愿意做的事情，他们都会一直支持我、鼓励我。没有他们的支持我根本无法完成。

我的孩子一开始对我经常没有时间陪伴她很不理解，有一次她同我讲起一个老师给她们讲的小故事，说姚明在他四岁生日时他的爸爸妈妈送给他一个篮球，后来

姚明就慢慢地爱上了篮球。我就立刻好奇地问孩子:“在爸爸妈妈每年送你的礼物中,有没有哪件礼物是你最喜欢的?或者对你意义最大的?”她的回答是我前些时间在她们学校做的一期讲座。这期讲座的主题是“小手机,大学问”,其中有一个研究的小节就是 NFC 手机是如何具有北京公交卡功能的。准备讲座期间,她陪着我一起准备手机样机、公交卡,以及设计 PPT 文件,就是在这个过程中让她了解了我大概在做些什么事情,我写的那本书是关于什么的。再后来她每次看到我在计算机前写东西,但又有事想打断我时,都会主动和我商量需要等待多长时间,然后她再过来找我。孩子开始懂事了,我想这既是动力也是对我最大的支持!

从书的构思、整理、申报、编写、校订,再到最后的出版,在这个过程中给予我支持的人很多,需要感谢的人和组织也特别多,在此特别感谢北航出版社、恩智浦(中国)管理有限公司、小米科技有限公司、华为北研、杭州雅观科技有限公司、Mobile CBG、一起走过的日子、This's best moment、老高和他的朋友们、gogogo Team Outing、乌兰布统休闲游,有了你们的帮助,使得本书能够顺利出版。

王晓华

2019 年 2 月 14 日

于北京市海淀区牡丹园

目　录

第1章 概 述

在一个NFC移动支付系统中，NFC主要负责通信部分，其中包括与外部非接触读头进行数据通信，以及把APDU数据转发到各种安全单元载体中；SE安全单元则主要负责实际支付的物理载体，其中包括硬件安全和软件系统安全等。关于前者的技术部分在《NFC技术基础篇》中已经做过介绍，所以本书的重点是介绍基于NFC技术的SE安全单元部分。

SE安全单元的范畴也是比较笼统的，有人把一些基于逻辑加密卡或者具备一些硬件加解密的芯片称为SE芯片，例如，有人把SIM卡片的芯片或者门禁卡芯片等叫作SE芯片。因为SE芯片是一个硬性翻译过来的词语，所以如果只是从字面上进行理解，那么把这些类似的芯片也称为SE芯片是没有问题的，但是这些具有全球统一的或者约定俗成叫法的，产品本身还是有很多区别的，如下：

首先，对于类似使用状态机机制等实现的逻辑加密功能的芯片，例如恩智浦公司推出的Mifare Ultralight和Mifare Classic等产品，它们虽然在硬件层面上支持3DES、Cryptol和AES等算法，但是对于用户接口而言，已经支持一些特定的私有指令集，芯片在接收到私有指令后，再做相应的加解密和支付行为处理；再如，Auth with Key A(0x60)、Auth with Key B(0x61)，以及Mifare Decrement(0xc0)、Mifare Increment(0xc1)等指令集在送到该逻辑加密芯片时，该芯片将通过原来设计好的逻辑处理流程，自动完成相关的加解密或者充值扣款的动作，而本身的逻辑处理并不可以修改或者进行二次编程处理。

其次，市面上还有一些加密芯片，它们可配合许多类型的微处理器芯片一起工作，为敏感信息提供永久的可靠性保护、物理保护机制和无痕迹存储器，有效保护敏感数据在遭遇物理攻击和篡改的情况下，进行即刻擦除外部存储器等保护处理。这种类似的加密芯片一般也会运行一段安全加密程序，但并没有任何的操作系统或者安全防火墙的概念，使用比较多的场景如在嵌入式系统中进行软件版权保护、物品配件或者辅料防伪鉴权、物联网联网安全证书校验等。对于这种类似的安全芯片，如美信半导体和国民技术等公司都有相关产品提供。根据行业的约定，并且为方便

介绍本书，就把此类芯片统称为原生码安全芯片。

在一些原生码安全芯片中，也会对 ISO/IEC 7816－4 中的文件系统进行相关实现，包括实现的根目录文件(Master File MF)、基本文件(Elementary File，EF)和专用文件(Dedicated File，DF)。其中，主文件或者叫根目录文件实际上就是专用文件的一种，这也是一个必须实现的文件。因为之后所有的基本文件或者专用文件都必须与根目录文件通过指针地址、数据链表或者特殊的数据结构连接在一起，除根目录文件外，其他专用文件都是可选项。

基本文件又分成两种类型：第一种为内部类型，主要存储的数据是可以通过安全芯片本身进行解释的，即数据的分析和使用过程都是在安全芯片下进行管理和控制的；第二种为工作类型，这些存储的数据本身并不能用安全芯片本身进行解释，只是提供给在外部应用所使用到的数据。如图 1.1 所示的逻辑文件的组织结构，其中，双长方形中的根目录文件是必选项，它的下面可以挂基本文件和专用文件，专用文件下又可以挂基本文件和专用文件，并且可以依次进行层叠链接。在这种类似的层叠链接层数过多之后，当想选择当前任何一层的文件时，可以通过如下方式进行：

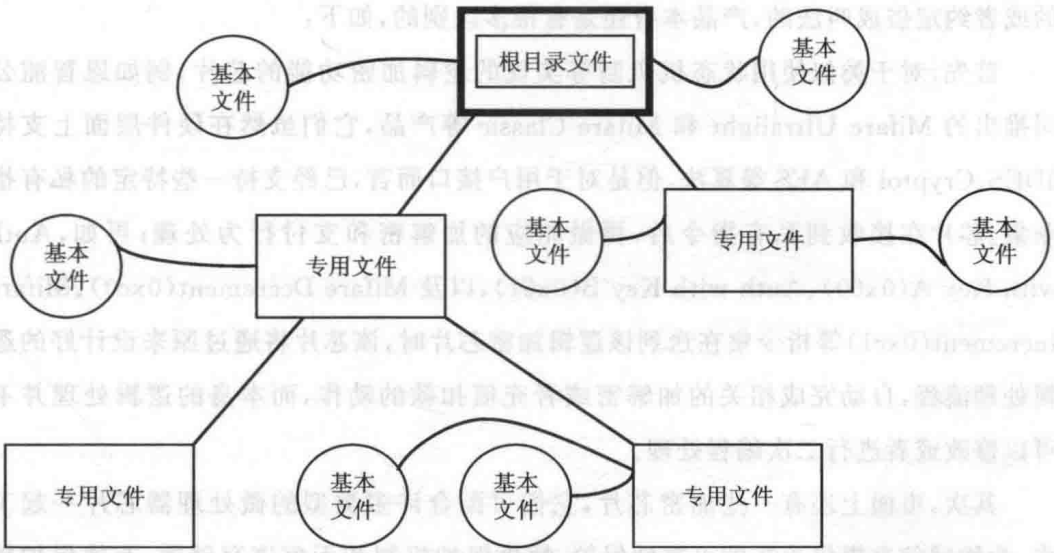


图 1.1　逻辑文件的组织结构

— 文件标识符方式(file identifier)；

— 来自根目录文件的路径(path from the MF)；

— 来自当前专用文件的路径(path form the current DF)；

— 专用文件的名称(DF name)。

对于具体的基本文件的实现，可以使用完全透明文件的格式，也可以使用线性固定或者 TLV 数据格式等。图 1.2 所示为当前主流的 5 种基本文件的数据格式。

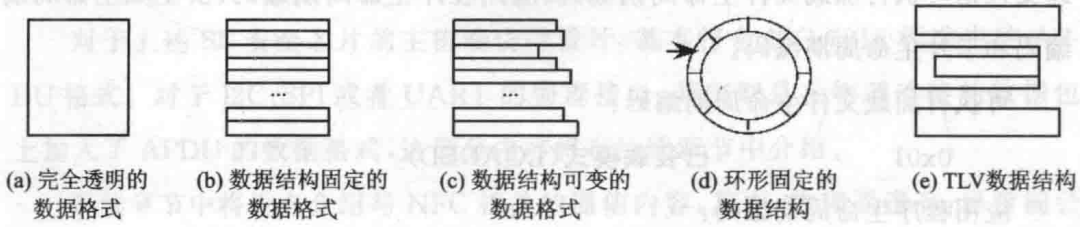


图 1.2 主流的 5 种基本文件的数据格式

第一种因为完全在一个数据容器里，所以不方便做索引管理，实际商用时使用得并不多；第二种由于其所有的数据结构体大小一致，所以有时会造成内存浪费；第三、四和五种是当前最主要的实现基本文件的数据格式，但在实际的商用部署中第三种和第五种是使用最广泛的。

对于此类安全芯片所包括的文件系统和数据结构，其主要的描述均在 ISO/IEC 7816－4 规范中，可以说，早期的 SE 安全芯片也都是从这个规格开始的。对于许多的 APDU 命令，其命令格式的 CLA 值以 0x0x 或 0x1x 开头的表示支持 ISO/IEC 7816－4 的命令，以 0x8x 或 0x9x 开头的表示专有命令，例如统一平台标准的命令(Global Platform，GP)。

最后一大类就是基于统一平台标准的安全芯片，这类芯片对比上面两大类：第一，提供了应用层程序以及统一标准化的编程接口，这样在调用不同的加解密算法时，有了灵活、标准化且统一的接口，方便上层应用程序的开发和应用；第二，在上层应用程序和底层硬件之间，有了操作系统和防火墙的概念和设计，对上层可提供相关内存管理、硬件加解密算法调用接口、应用和安装管理等，对下层最主要的功能就是实现了应用处理器跨平台处理的功能，实现了 Java 字节码解释器的功能；第三，还有特别重要的一层，就是对产品从硬件、操作系统、防火墙子系统和应用程序等方面提供了生命周期管理的概念，这样在某种意义上算是真正地实现了硬件安全的设计；第四，对于整个芯片硬件、操作系统和应用等，提供了一整套的安全测试规范，其宗旨是为了让搭建的整个系统达到安全标准的等级，使最终实现通过验证的整套硬件产品可信赖，并且它是支持统一平台标准的。

这里介绍的统一平台标准以及 Java Card API 标准，对于基于 SE 安全芯片开发的程序而言就是最主要的接口，接口主要包括编写 Applet 时的接口，其生命周期管理又包括可执行加载文件生命周期编码、应用程序生命周期编码、安全域生命周期编码和卡片生命周期编码。

可执行加载文件生命周期编码：

0x01	已装载模式(LOADED)

应用程序生命周期编码：

0x03	已安装模式(INSTALLED)
0x07	可选择模式(SELECTABLE)
0x07～0x7F	应用程序的特定状态(Application Specific State)
0x83	已锁定模式(LOCKED)

安全域生命周期编码：

0x03	已安装模式(INSTALLED)
0x07	可选择模式(SELECTABLE)
0x0F	已个人化模式(PERSONALIZED)
0x83	已锁定模式(LOCKED)

卡片生命周期编码：

0x01	运行环境准备就绪状态(OP_READY)
0x07	已初始化(INITIALIZED)
0x0F	安全模式(SECURED)
0x7F	卡片锁定模式(CARD_LOCKED)
0xFF	生命周期终止模式(TERMINATED)

生命周期管理可以说是 SE 安全芯片的一个重点，后续章节将对该内容进行比较详尽的总结和说明。

本书将用少量篇幅来介绍逻辑加密芯片和原生码安全芯片的基本原理，用大量篇幅来介绍统一平台标准的安全芯片。其中，还有一主要内容是介绍统一平台标准的安全芯片与 NFC 射频前端控制器之间的通道数据问题，对于 SE 安全芯片，其实完全可以设计成一个独立运行的 SE 芯片小系统，直接与微控制器进行通信。实际上，在许多电路设计中已有相关的应用案例，例如，Apple Watch 3 中关于 eSIM 的设计，就使用了一颗由 ST 意法半导体公司生产的 SE 安全芯片；金雅拓 Gemalto 的 SE

安全芯片，赢得了微软平板电脑市场；谷歌公司的 Google Pixel 2 和 Pixel 2 XL 支持 eSIM 功能。这些安全芯片本身并不与 NFC 直接连接，但是它们与主机端系统通过 I2C、SPI 或者 UART 的物理接口进行连接。

对于上述 SE 安全芯片的主机端访问设计，基本符合 ISO 7816 标准中的 APDU 格式。对于 I2C、SPI 或者 UART 的物理接口，其实就是在物理连接的数据包上加入了 APDU 的数据格式，这部分内容将在后续章节中介绍。

后续章节中将重点介绍与 NFC 相关的通信内容，其中，物理通道有：恩智浦公司的模拟信号接口（Sigin-Sigout-Connection，S2C），该接口进入国际标准后，公开的标准名改为 NFC 有线接口（Near Field Communication Wired Interface，NFC-WI）；英飞凌公司的数字非接触式桥接口（Digital Contactless Bridge，DCLB）复旦微电子曾主推过的增强型单线接口（enhanced Single Wire Protocol，eSWP），其原理就是在使用传统的 SWP 物理单线接口的基础上，把其分成电流和电压两根物理线路进行通信。当然，还有许多其他的物理连接接口，表 1.1 所列为 NFC 与 SE 安全芯片之间的部分安全物理通道。

表 1.1 NFC 与 SE 安全芯片之间的部分安全物理通道

安全物理通道	说 明
SWP(Single Wire Protocol)	参考规范《ETSI TS 102 613》
eSWP(enhanced SWP)	复旦微电子的私有规范
DWP(Dual Wire Protocol)	恩智浦公司的私有规范
DCLB(Digital Contactless Bridge)	英飞凌公司的私有规范
ACLB(Active Contactless Bridge)	奥地利微电子公司的私有规范
NFC-WI(Near Field Communication Wired Interface)	参考规范《ISO/IEC 28361》或者《ECMA - 373》
S2C(Sigin-Sigout-Connection)	参考规范《ISO/IEC 28361》或者《ECMA - 373》

对于表 1.1 所列的物理通道部分，本书不做过多介绍，但是，对于其通信管道的建立，将进行相关的案例分析和示例介绍。

对于 SE 安全芯片的操作系统和应用程序的原理和示例，本书将用少数章节进行介绍和讲解；另外，对于统一平台标准和 Java Card 标准接口，本书也将用少量的章节进行介绍。如果想要了解更多的细节，则可进入官方网站搜阅相关资料。

关于书中多种加密算法的具体算法的原型和实现可以参考相关资料，本书之所以设置相关章节，是为了阅读的连贯性和必要性，因为在后续章节中需要相关的技术支持。比如，在 SE 安全芯片中建立安全通道，它就使用了许多加密算法，这可能也是 SE 安全芯片中一个最主要的技术板块。