NFC, Smartphones and Libraries – A Turning Point

Introduction

Back in February 2013, we issued a comprehensive newsletter piece about NFC. Even if you read that newsletter, still keep on reading this paper. As matters have progressed, we have decided to update the content whilst still retaining some of the original material. This particular paper goes into a lot more detail and provides some current facts.

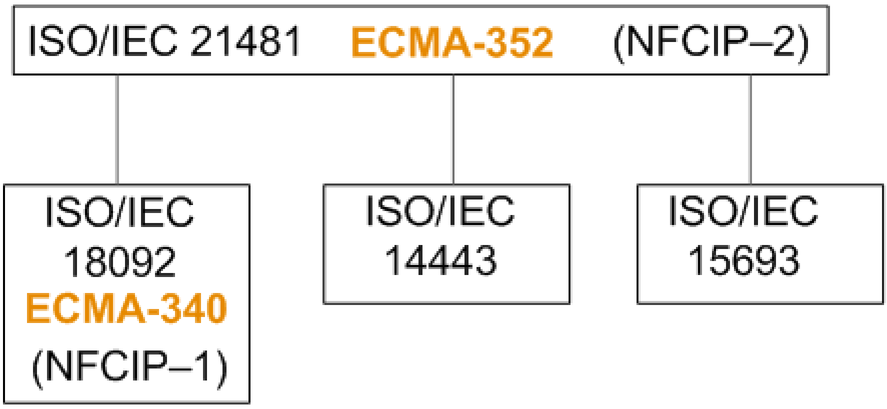
There has been a lot of confusion about NFC and libraries

Originally, NFC (Near Field Communication) was a specific extension to smart card technology that used a variant air interface protocol (i.e. the means of communication between the reader and the tag). Without getting too technical, using this modified protocol NFC-enabled smartphones were able to act as readers and even be emulators of tags. The NFC Forum developed four specifications; three being an extension of ISO/IEC 14443, and the fourth one based on the Japanese FeliCa standard. All of these operate at the high frequency of 13.56MHz. The NFC Forum also developed various well-defined message structures.

A few years ago, all of this meant that:

- NFC and RFID in libraries used different air interface protocol. There was no conflict with libraries that were using ISO/IEC 18000-3 Mode 1 tags (based on the inherent ISO/IEC 15693 protocol).
- The different NFC data structure also meant that there was no conflict with ISO 28560 and even any proprietary encoding rules.

Then it all changed. Along came a new standard, originally specified as ECMA-352[1] in 2010 and then published by ISO as ISO/IEC 21481:2012. This standard defines the rules for a high level protocol selector. It is formally known as NFCIP-2 and specifies the communication mode selection mechanism between different air interface protocols, as shown in the figure:


ISO/IEC 21481 ECMA-352 (NFCIP–2)
ISO/IEC 18092 ECMA-340 (NFCIP–1)
ISO/IEC 14443
ISO/IEC 15693

The protocol selector enables the device to work in one of four modes:

- Support the original NFC protocol[2], with its own security and message structures
- Read and write ISO/IEC 14443 smart cards
- Act as an emulator of a 14443 smart card
- Read and write to the ISO/IEC 15693 protocol, and therefore to ISO/IEC 18000-3 Mode 1

[1] http://www.ecma-international.org/publications/standards/Ecma-352.htm. This was updated in 2013

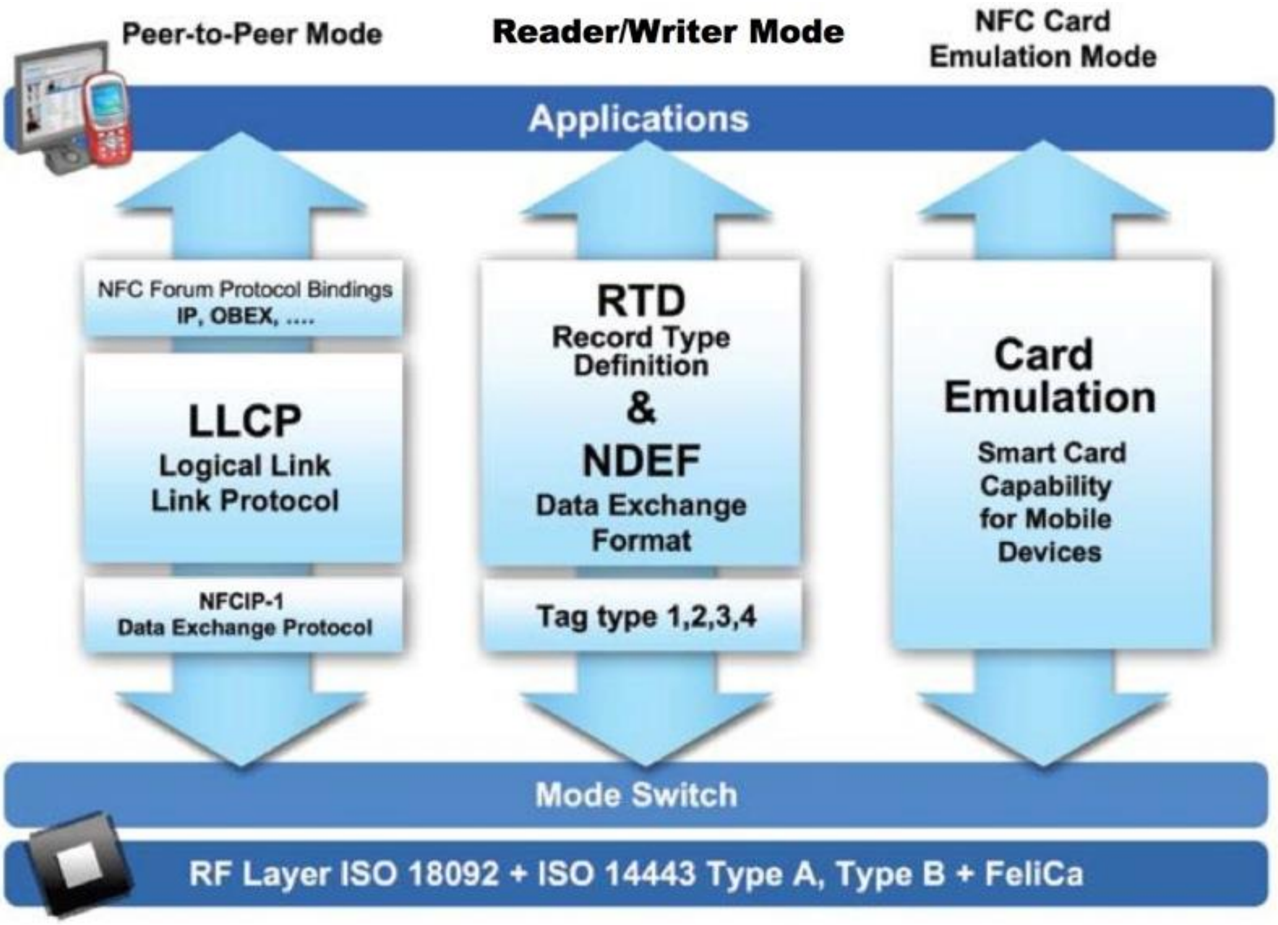
[2] ISO/IEC 18092 (or the equivalent ECMA-340)

It is this last point that has the biggest impact on libraries, although there are some implications from the fact that NFCIP-2 also supports the more general features of ISO/IEC 14443.

In February 2013 the NFC website supported a section on FAQs (it no longer seems to do so). Under the heading '**What ISO/IEC standards do the NFC Forum specifications support?'** The answer was:

> NFC Forum compliant devices in NFC Forum reader/writer mode must support the RF requirements of ISO/IEC 14443A, ISO/IEC 14443B and FeliCa as outlined in the relevant parts in ISO/IEC 18092.

This figure, from the NFC Forum website[3], shows the architecture and what features are formally supported:


Peer-to-Peer Mode
Reader/Writer Mode
NFC Card Emulation Mode
Applications
NFC Forum Protocol Bindings IP, OBEX, ...
LLCP
Logical Link Link Protocol
NFCIP-1 Data Exchange Protocol
RTD
Record Type Definition
&
NDEF
Data Exchange Format
Tag type 1,2,3,4
Card Emulation
Smart Card Capability for Mobile Devices
Mode Switch
RF Layer ISO 18092 + ISO 14443 Type A, Type B + FeliCa

There is no mention of support for ICO/IEC 15693 in the figure or the list of NFC Forum Specifications[4].

The conclusion that we reach is that ECMA-352 (and later ISO/IEC 21481) are the result of technology enhancements driven by manufacturers of integrated circuits, probably to increase the potential market for devices and applications. **But, as usual with the laws of unforeseen consequences, the capability of**

[3] http://nfc-forum.org/our-work/specifications-and-application-documents/specifications/

[4] http://nfc-forum.org/our-work/specifications-and-application-documents/specifications/nfc-forum-technical-specifications/

reading tags complaint with the ISO/IEC 15693 protocol is that certain NFC reading devices can actually read and even write to tags used in libraries.

Market Data

We have identified some sources of data. Wikipedia provides an interesting annual sales table[5] showing the rise and fall of different operating systems from 2007 to 2013, with some limited data for the current year. In 2013 the sales were:

Android	759 million
iOS	151 million
Windows	31 million
Blackberry	19 million

There is also data about the installed base, which provides a better picture of the potential impact of NFC-enabled smartphones.

Installed Base of Smartphones by Operating System as of 30 Sept 2014

Rank	OS Platform	Units	Market Share		Main Manufacturers
			Q3 2014	Q2 2014	
1	Android	1.455M	74%	72%	Samsung, Huawei, Sony, Lenovo, ZTE, LG, Coolpad, HTC, Xiaomi, Motorola/Google
2	iOS	373M	19%	19%	Apple
3	Windows Phone	59M	3%	3%	Nokia/Microsoft, Samsung, HTC
4	Blackberry	38M	2%	2%	Blackberry
5	Symbian	27M	1%	2%	Nokia
	Others	8M			
	Total installed base in use	1966M			

Source: Tomi Ahonen Consulting Analysis 7 November 2014, based on manufacturer and industry data[6]

In his blog article, Tomi Ahonen states that there were 320 million smartphones sold in Q3 2014, which is 23% up on the same quarter in 2013. The data from the Wikipedia page[5] has sales of 262 million for Q1 2014. An interesting fact is that the data from Tomi Ahonen shows a difference between the sum on the units and the total installed base of 1966 million. On other pages he shows an installed base of 1748 million for Q1 2014. All this data reflects that while the total installed base is increasing, there is a level of attrition probably due to older smartphones being replaced by newer models.

It is clear that smartphones based on the Android operating system dominate the market, with Apple's phones coming second but a long way behind. It is difficult to ascertain from these broad market share figures which phones support NFC and which do not. A useful source of information is a list provided by NFC World[7]. When we looked at the list over a year ago, it was significantly shorter. We have tried to check out the data sheets and technical specifications for some of the phones, but the majority just indicate that they support "NFC" without distinguishing between the original basic NFC functionality and that supported by chips that support ECMA-352 compliant products. In fact, simply indicating that a product complies with ECMA-352 only confirms that a front-end switching mechanism is supported. What the chip

[5] http://en.wikipedia.org/wiki/Smartphone [Accessed 2014-11-28]

[6] http://communities-dominate.blogs.com/brands/2014/11/index.html

[7] http://www.nfcworld.com/nfc-phones-list/#ringers

needs to support is a completely integrated set of air interface protocols as is the case with the multi-protocol fully integrated 13.56-MHz RFID/NFC Transceiver IC (TRF7970A) available from Texas Instruments[8]. As a chip like this costs less than 7 USD, it is easy to see how it can easily be incorporated into an expensive smartphone.

What are the good, the bad and the ugly features of these developments?

The first thing to say is that it is not all bad, but some of the aspects of this development are complex. If we start with a positive, this means that patrons with smartphones that support NFCIP-2 readers might be involved as stakeholders with new services offered by the libraries. A risk we see is that such developments might be haphazard, whereas a co-ordinated approach might yield better results.

The "bad" is that such readers look just like normal smartphones, but might be used for some occasional reading and even writing new and different data to the tag.

The "ugly" could result in a concerted attack on tags, which would effectively be a new type of denial of service attack achieved by corrupting data from one or many tags.

We briefly look at each in turn.

New library services

A number of companies are developing solutions on smartphones to offer to libraries. As Convergent Software is not a hardware supplier, we will be fairly brief on this particular area of development. In addition to the development of multi-function reader chips, there has also been a growth in the number of other chips that can add security such as *secure element* chip. There are also protocols that support authentication. Libraries should consider two broad types of application.

Where the device is fully owned by the library, whether with an application on a smartphone or a more sophisticated personal digital assistant (PDA), the library management should ensure that the specification of the product and the communication protocol is as secure as possible. This includes protection against features such as eavesdropping on the RFID communication.

The situation is more complex when a service is opened up to patrons, using their own devices. The most obvious operational constraint at present is that the NFC functionality supported by Apple phones is either limited to contactless payment or non-existent on models older than the Apple iPhone6 or Apple iPhone6 Plus. But the complexity is just as bad for Android and Windows phones where support for the feature is not openly declared.

Smartphones that only support the original ECMA-340 functions can still be used as smart card emulators and, of itself, this could change the basis for ‘issuing’ membership cards. Smartphones that support the functionality of ECMA-352, in other words the reading and writing of ISO/IEC 18000-3 Mode 1 tags (with the inherent ISO/IEC 15693 protocol) need to be handled extremely carefully. We discuss some of the issues below. For now, consider the situation where a library decides the smartphones can be used as a membership card emulator, and a number of patrons discover accidentally or deliberately that they can also read and write to the RFID tags held on loan items. If not handled correctly, this could have potential for a lot of problems for the library.

[8] http://www.ti.com/product/trf7970a

Whatever decisions are made about allowing patrons to use smartphones for membership card emulation or for reading tags on books, considerable care should be taken to ensure that a reasonably high level of security is supported. This is something that every library management needs to discuss with prospective suppliers of solutions.

The bad and ugly from an operational perspective

We leave the reader to decide which of the following points fall into the category of bad or ugly. It is probably a question of scale and even detection that something might not be right.

Let's start with a patron using a smartphone for reading a tag on a loan item. If this is part of an intended service such as self-checkout, check-in or being able to compile a prospective reading list, then this would not appear to be a problem. But if it is possible to read one or a few tags, it might be possible to read many tags and create what NISO has called a *hot list*, which might later be used to read tags outside of a library environment. This begins to impact on privacy, which we discuss a bit later. Also bear in mind that to read any data from the tag there is a fundamental requirement to first read the chip ID. If these chip Ids are stored, it makes monitoring outside of the library somewhat easier. It just requires the minimum of RFID knowledge to do this.

While the intention of a library might be to not permit a patron to write data to the tag, it is impossible to prevent this on any smartphone that has the capability of supporting the inherent ISO/IEC 15693 protocol. It does not matter whether the library has implemented an application using smartphones; just having them on the premises does present a marginal risk. When this was discussed at the ISO Technical Committee meetings, one of the university librarians expressed concern that once tech-aware students made this discovery, then there could be a wider implementation of changing data on the tag.

We have also seen a misunderstanding by some in the library community about the way RFID works. While at one level there are sophisticated data protocols such as ISO 28560-2, where externally meaningful data is manipulated to be encoded on the tag and the reverse manipulation has to be applied on decoding, what is transmitted across the air interface is significantly simpler. There are three areas of concern:

1. Most, but not all, tags transmit data in 32-bit blocks. This applies to reading and writing. So all that needs to be done to corrupt the data on the tag is to read the first 32 bits, change a few bits and then render the tag unreadable.
2. The Data Storage Format IDentifier (DSFID) is an 8-bit byte on the tag and has an explicitly defined command to write its value to the RFID chip memory. The DSFID often declares the encoding rules for the rest of the data on the tag. So if any single bit is changed, it might make it difficult for the system to interpret how the rest of the memory is encoded.
3. The Application Family Identifier (AFI) is also encoded as an 8-bit byte and there are read and write commands for this. In many libraries, the AFI value is toggled between two defined values to indicate an in-stock or checked-out status. Depending on how the security gate systems are set up, changing the AFI randomly might result in a lot of alarm signals, or changing the "in-stock" setting to "checked-out" without going through the formal checkout procedures could mean that someone leaves the library with a loan item that *appears to be checked out* but the LMS/ILS still shows it as in stock.

Whilst various people claim that none of this has happened in libraries, possibly so far, there is no way to prove that this has not happened. This is the classical *Black Swan* logic problem: that until evidence is found of a black swan existing, the claim can be made that it does not. The scale, in terms of monetary value of walking out of a library with a loan item and not returning it is not dissimilar to manipulating a lowcost travel card to get free trips on a public transportation system. A recent story from the security company Trend Micro identified a high-risk Android app in Chile that was being distributed through social media that can hack into the user's RFID public transport card to re-charge the credits. Let's put this into perspective. The transport card being used in this hack actually supports encryption overlaid on top of an ISO/IEC 14443 chip. The detailed article[9] from Trend Micro shows that the tag memory needed to be analysed defined the area in memory to change the monetary value. None of the RFID library protocols using the inherent ISO/IEC 15693 protocol support encryption. It only requires the use of standard air interface commands to manipulate the data on a tag on a library loan item. **In other words, it would be significantly easier to develop an Android app that could distort the encoded data on the tag.** We have been deliberately coy about explaining how this could be done, but it requires less sophistication than even that required for the most basic encoder.

Let's consider how to mitigate against the three types of data distortion:

1. If there is any bit-based distortion, the data element that will cause most harm is the Primary Item Identifier (or bar code number). In ISO 28560 standards, this is encoded in the first part of the memory. Therefore, if the lower memory locations are locked, then only optional data might be damaged. Any hacker would really need to know something about the library RFID standards just to change that data, and it would also take longer to do. Of the library encoding schemes, ISO 28560-2 is best placed to deal with this because it has been designed to support selective locking. Other library encoding schemes provide an "all or nothing" approach to locking data. By selectively locking the primary item identifier and leaving other data elements unlocked, a library gets the best of both worlds. It protects the tag from being rendered unreadable, but still leaves the rest of the memory open for additional data to be encoded. Now is the time to think seriously about converting existing RFID solutions to ISO 28560-2.
2. Locking the DSFID would be a fairly sensible operational decision. Once encoded, it effectively becomes read-only. The only situation when it should not be locked is if the library plans to migrate to ISO 28560-2, in which case the DSFID should not be locked until the tag has its data encoding converted.
3. Addressing what to do with the AFI is a bigger challenge. Any library that toggles the value of the AFI between the "in-stock" to the "checked-out" state cannot lock the AFI if this is the means of achieving control at the security gates. However, there are other ways that the security gate system can be implemented which will enable the AFI to be locked. We won't go into details here, because there are various factors to consider. However, we are prepared to discuss the options either with RFID system vendors or individual libraries. The solution might require changes to software, but could be completely transparent to patrons. Most importantly there is no requirement to change any tags.

The bad and ugly from a privacy perspective

One of the comments sometimes made about the use of NFC is that the read range is very short. Therefore, the argument continues, there are no privacy risks. If this is true, then using an NFC-enabled smartphone to read data from an RFID tag would be quite limited. However, there have been enough reported cases where contactless payment cards have responded at greater distances than the intended few centimetres for the claim of limited read range to not hold true in all circumstances. In fact, only this month it has happened to us, when payment was taken from a card from about 30cm away when our preferred option was to use the chip and pin facility.

[9] http://blog.trendmicro.com/trendlabs-security-intelligence/hacking-rfid-payment-cards-made-possible-with-android-app/

There are promotional videos (we are not providing a link because they are designed to sell card shields) where a 'privacy expert' walks around a busy location with lots of people, reads their smart cards and shocks them when he shows them basic information extracted from their cards in their pockets, handbags or wallets. It is important to understand the technology that lies behind this. A smartphone with the relevant app can read any 18000-3 Mode 1 tag within reading distance and simply dump the encoding in memory for later analysis. Any means of boosting or maintaining a smartphone to full battery capacity – of which there are portable solutions on the market, some that are small yet can keep a phone at full power for ten times the internal battery power – can turn the smartphone into a reasonably powerful data capture device.

Within the last year or two, devices have come on the market that link a front end antenna, the part of the system that sends the signal to the RFID tag, to a main reading device and decoder such as a smartphone with the appropriate NFCIP-2 reader chip. This just requires the antenna to be coupled to the smartphone using an appropriate port. The antenna can easily be concealed and be powered separately from the smartphone, which simply processes the captured RFID data. In this type of case, the smartphone battery is not used to read the tag, just to store or decode the data that is read. Libraries might even be offered commercial products that do this so that the smartphone can be used as a *store, process and forward* device for inventory purposes.

Currently, there is no assured way to stop the elicit reading of RFID tags that use a basic RFID protocol like ISO/IEC 18000-3 Mode 1 in the *uncontrolled domain* beyond the perimeter of a library. There is always a privacy risk and Convergent Software has released a separate paper about RFID privacy describing the European approach to undertaking an RFID privacy impact assessment.

Summary

The rapid take-up of NFC-enabled smartphones is clearly set out in some of the facts presented in this paper. With over 1.5 billion devices – and growing – smartphones on the market are most likely to support NFC. Libraries need to take some interest in the potential benefits and problems that can arise from this technology. There is certainly scope for innovation to develop new services.

There is a risk to core operations because data can be manipulated on an RFID tag. There are ways to minimise these risks and we would be happy to discuss this with anyone with a serious interest in the issues. Contact us at nfc@convergent-software.co.uk

The risks of elicit reading, and thus creating potential privacy problems is more difficult to eliminate. In an associated paper we discuss some of the issues about privacy.

In all cases, we will discuss any of the issues on a confidential basis either with existing clients, vendors or libraries.