NFC equipped smartphones: a two-edged sword for library RFID systems

Alan Butters
Principal Consultant, Sybis
alan@sybis.com.au
www.sybis.com.au

Abstract
The last few years have seen a significant increase in the number of smartphones equipped with Near Field Communication (NFC) capabilities. NFC utilises several technologies that will allow a user's smartphone to interact with a range of other devices in ways that further expand the smartphone's utility and capability. The technology paves the way for smartphones to interact both positively and negatively with library RFID tags. This paper outlines the capabilities and penetration of NFC-equipped smartphones, and discusses a range of mitigation strategies that might be available to libraries where the threat aspect of NFC is of concern.

Introduction

The topic of Near Field Communications (NFC) equipped smartphones and their potential interaction (both positive and negative) with library RFID systems is a complex one. The topic is complex not simply because of the technology involved, but also because of the range of interactions that are possible. Libraries may also have broadly differing views as to the seriousness of the actual threat posed by smartphones and the extent to which mitigation strategies are required. With this in mind, an attempt has been made in preparing this paper to be strictly analytical when articulating the possible negative interactions between the two technologies and to allow the individual reader to assess the seriousness of the risk and its likelihood of occurrence within their own domain.

The paper is best read as a starting point for further discussion. It is likely that libraries or groups of libraries will take different approaches to potential smartphone threats and there is no reason why this should not occur. However, in libraries where a threat is assessed as being significant enough to warrant a mitigation strategy, it may be useful to broaden the discussion, in order that leverage might be gained by a cooperative approach, particularly where an RFID supplier's assistance is needed.

The aim of this paper is to:

- Provide informative material to assist library managers and others to understand (NFC) technology and its capabilities.
- Provide a market snapshot of NFC-equipped smartphones and tablets currently available that have the capability to interact with library RFID systems.
- Provide an overview of both the opportunities and the threats to library RFID systems brought about by the proliferation of NFC-equipped smartphones.
- Articulate a range of specific threats and possible mitigation strategies, intended to form a basis for discussion within the library community and with library RFID suppliers.
- Encourage subsequent discussion of the issues raised in this paper to also focus on preserving the interoperability benefits now being delivered by ISO 28560.

Brief overview of NFC technology & applications

For the purposes of this paper, we will consider NFC to be a kind of RFID, not dissimilar to the technology by means of which many libraries have automated a number of circulation processes (Finkenzeller 2012). The term NFC may apply to NFC tags, which are passive devices without a power source and similar to library RFID tags, or smart NFC devices such as Point of Sale readers or smartphones, which are active devices capable of generating their own Radio Frequency (RF) field.

Building NFC capabilities into smartphones allows for a range of new and innovative applications to be developed, which is why nine out of ten of the leading smartphone manufacturers are now shipping their devices with NFC capability (Ranger 2013). As the name suggests, NFC operates in the near field: typically up to ten centimetres, but often much less. For this reason, NFC is often described as a “tap and use” technology (Infineon 2013). Contexts can include:

- Tap and go: ticketing systems etc
- Tap and confirm: payment confirmation etc
- Tap and capture: obtaining information etc
- Tap and link: linking to external data sources or storage
- Tap and connect: sharing data between two NFC devices
- Tap and explore: a combination of these contexts

NFC has three basic operating modes (Vedat 2012):

- Reader / Writer mode
- Peer-to-Peer mode
- Card Emulation mode

Perhaps the easiest way to understand what the NFC-equipped smartphone might be used for is to present a number of application examples. An example will be provided for each of the three modes.

Reader / Writer mode

As suggested by the name, this operating mode concerns communication between an active NFC device and a passive NFC tag. This mode is very similar to the operating mode within a library RFID system where an RFID reader either reads an RFID tag (such as might occur in an inventory context using a handheld device) or writes to the tag, as during circulation processes where the tag’s security status is updated.

An example of NFC in reader / writer mode is the smart poster. In this case, an NFC-equipped smartphone acting as a reader is placed against a specific location on the poster, where it can read data from an embedded NFC tag. By this action, an application on the smartphone might be triggered and the user could be prompted to buy tickets to an event, could be invited to download a music sample or could be taken to a specific website.

This same mode could be used with public transport route maps, where touching the desired destination name automatically transfers the details of the timetable to the smartphone. Touching an NFC-equipped menu in a restaurant may also enable a diner to transfer reviews or location details to friends by integration with a range of social networking applications.

Peer-to-Peer mode

In this mode, NFC devices are connected wirelessly for the purpose of the controlled exchange of information, or an NFC device is connected to an external resource over the Internet. An example of this might be the exchange of electronic business cards and other contact information. As NFC devices are able to initiate communications, all that may be required is for two smartphones to be touched together to begin the sharing process. The user may then be prompted to accept the sharing of contact details and the exchange takes place. The same methodology could be used in a range of social media contexts where, for example, requests to be friends might be initiated seamlessly.

Card Emulation mode

This mode allows an NFC-equipped smartphone to function as a contactless smart card. In this context, the smartphone is used to interact with an NFC reader. This mode opens up a great many potential applications such as:

- Payment: the smartphone may be used instead of (by emulating) a credit card or debit card or gift card etc. In this way, the smartphone becomes a kind of electronic wallet, replacing a number of plastic cards.
- Access control: the NFC-equipped smartphone may be used for a range of purposes such as building entry, vehicle keyless entry etc. It is also possible to construct a system in which a hotel access key is transferred to the smartphone in advance of a guest's arrival. The smartphone could then act as a wireless access card to gain access to the room. In this way, the guest may arrive after hours or at time when the reception is desk closed. It may also remove the requirement to manually check-in at all when arriving at the hotel.
- Ticket management: many tickets could be incorporated into the NFC-equipped smartphone, including cinema tickets, public transport tickets, airline tickets and concert tickets. It could also be possible to purchase event tickets from an advertising poster using the smartphone and then to gain entrance to the event immediately after by using the same device.
- Identity information: there is potential to shift the storage of personal information from an existing computer database to an NFC-equipped smartphone, thereby placing control of the personal information in the hands of the user. Such information might include personal medical information that the user may elect to share with a third party such as a healthcare professional by means of a fixed NFC reader.
- Environment control: the applications in this area relate to the personalisation of a user's office or home environment by means of the NFC-equipped smartphone. A user could customise a number of factors such as temperature, lighting or music by touching the smartphone to a wall mounted reader, or even at the point of entry when using the smartphone to gain access to a room.

NFC & library RFID standards

The NFC technology platform is built on a range of commonly used standards and readily available products. Where reading and writing of passive NFC devices (tags) is concerned, the NFC chips that are integrated into smartphones support a range of air interface standards and two of these are summarised below.

ISO 14443

This is a short-range contactless smartcard standard often used in ticketing systems for public transport users. The most widely used example is the MIFARE card, owned by NXP Semiconductors, which represents approximately eighty per cent of contactless smartcards used in the world. The Australian MyKi travel card system also employs technology based on ISO 14443, as does the London Transport Oyster card.

ISO 15693

This is the standard upon which all high frequency library RFID systems are based, and permits a read range of typically seventy centimetres or so. The standard defines how an RFID reader and an RFID tag will communicate, and includes a range of commands and responses that may be used in constructing an RFID software application. Interestingly, ISO 15693 is not actually part of the formal NFC specification, and so strictly speaking should not be referred to as NFC. However, NFC controller chip manufacturers are including support for this standard in their chips, as it opens up a number of longer-range applications for smartphones. Therefore, while arguably not technically correct, this paper will refer to all of the capabilities of smartphones and tablets, including support for ISO 15693, as NFC.

Of these two standards, ISO 14443 has received the greatest support by NFC chip manufacturers to date. It is used in many applications and offers security capabilities not found in ISO 15693. Smartphones supporting ISO 14443 have been available for many years. An important point to keep in mind is that the extent to which NFC-equipped smartphones have the potential to interact with library RFID tags (both positively and negatively) will largely be determined by how many smartphones are released with the hardware and software capability to read from and write to ISO 15693 tags. smartphones capable of reading and writing only to ISO 14443 tags cannot interact with library RFID. It should also be noted that at this time no NFC-equipped smartphone is capable of interacting with the UHF tags utilised in some library RFID systems.

Therefore, the two dimensions to be considered in the library context are:

1. The number of ISO 15693 capable smartphones in existence at a given time.
2. The plans for future smartphone models that may support ISO 15693.

As an indication of the former, chipmaker NXP Semiconductors, the largest supplier of NFC controller chips, shipped 125 million NFC chips for smartphones during 2012 (Balaban 2013). These chips support reading from and writing to high frequency library RFID tags. In fact, NXP offers a free app capable of writing to ISO 15693 tags.

NFC smartphones available now to library users

There are many lists of smartphones available from magazines and Internet resources, such as CNET Australia, PC World Australia and SD Net Australian Edition. Such lists, aimed at prospective purchasers, include smartphones that are described as most-popular, best-selling, best-performing and so on. While the lists to some extent represent subjective assessments, a number of devices are common to such lists, and it is useful to consider these newer and popular smartphones in the context of NFC and library RFID systems. The following is a table containing NFC-equipped devices available for purchase as of September 2013, and which have achieved broad popularity. Where ISO 15693 is supported, typically the only NFC mode included is Reader / Writer mode.

Smartphone	OS	NFC Chip	14443	15693
Apple iPhone 5	IOS	None	N	N
Google Nexus 4	Android	Broadcom	Y	Y
HTC One X/XL	Android	NXP	Y	Y
LG Optimus G	Android	NXP	Y	Y
Motorola Droid Razr	Android	NXP	Y	?
Nokia Lumia 920	Windows 8	NXP	Y	Y
Samsung Galaxy Note II	Android	NXP	Y	Y
Samsung Galaxy S III	Android	NXP	Y	Y
Samsung Galaxy S 4	Android	Broadcom	Y	Y
Sony Xperia S	Android	NXP	Y	Y

The table above demonstrates that most of the popular devices in the market have the technical capability to read from and write to library RFID tags. Just one smartphone model from the list, the Samsung Galaxy S III, was reported to have sold over fifty million units since its release, and its replacement, the S4, is projected to reach one hundred million in unit sales (Petrovan 2013).

It should also be noted that while a particular NFC device has the capability to read and write ISO 15693 tags, the device may not be supplied with an app to facilitate this. In terms of software apps that are available to take advantage of the NFC controller chip fitted to the devices in the list, hundreds of such apps exist already, although most are not aimed at ISO 15693 tags. *NfcV-reader* is an example of a free app that is capable of overwriting library ISO 15693 tags. In addition, given NXP's dominance in the Android-based smartphone market, should a library-targeted app be developed, it could be made available to a very large percentage of smartphone users exceptionally quickly.

In addition, a number of software tools exist for developers and others wishing to create their own apps. There are NFC software "stacks" available that are software modules allowing the development of new NFC apps. There is an Android NFC stack that permits direct access to ISO 15693 air interface commands and also an Open NFC stack that potentially allows direct access to the NFC controller chip.

While the Apple iPhone is conspicuously absent from the NFC smartphone list at this time, third party NFC devices such as the Flojack and FloCase or the iCarte are

being offered to provide Apple products (and older Android smartphones) with NFC capability. All products mentioned support ISO 15693, and the iCarte product is supplied with an app that allows the rapid overwriting of all memory blocks in ISO 15693 tags. Many industry commentators appear to expect an Apple smartphone with native NFC capability in the near future.

Opportunities for NFC in libraries

Self-Service circulation

At the moment, user self-service is generally accomplished by purpose-designed kiosks, and for many libraries this will continue to be the preferred way to loan and potentially return library material, particularly where large numbers of items are concerned. However, there are likely to be users, perhaps academic library users borrowing only one or two items, who would prefer to issue the material to themselves using a smartphone NFC app and the library Wi-Fi network.

If the app is configured with the library ID of the user, there would be no need even for a library card. Such an app, being installed on a private phone, could also provide a range of other user benefits such as recording due dates and reading history, and displaying recommendations and reviews.

Improved customer service

In a library employing an RFID infrastructure, staff equipped with ISO 15693 capable smartphones would be able not only to find a specific item for a user but also to issue the item on the spot, perhaps with an email receipt. While portable circulation tools are already available in the market, they are significantly more expensive than a smartphone. As the smartphone also has a cellular connection, it may similarly be used onsite in a home services context, in contrast to most purpose-designed portable circulation devices that are limited to Wi-Fi enabled locations.

NFC-equipped smartphones could also open up user-initiated activities such as a variation of the Danish Aarhus libraries' Bib-phone concept (Lykke-Olesen et al 2007) where children use a specialised RFID / Wi-Fi device to leave and retrieve verbal reviews for popular library material.

Integration with other smartphone apps

Smartphones continue to grow in capabilities, and there will be an almost endless list of synergies to be achieved with an NFC library app and other applications running on the device, for example:

- Integration with social media applications to allow an item with an RFID tag to be read, and reviews and recommendations from individuals known to the user to be retrieved.
- Ability to download data over Wi-Fi from NFC-enabled library promotional signs within the library, such as new releases, best sellers and prize winners. Optionally be able to parse these lists through local preferences, favourite authors or social media recommendations.

NFC & library RFID system vulnerabilities

One of the challenges for libraries in this context is that ISO 15693, the High Frequency RFID standard to which tags used by most libraries conform, was not designed with data security in mind. In addition, the standard itself is almost fourteen years old: a considerable age in a dynamic technology environment. While the standard has been embraced more recently as part of the ISO 18000 family, the essential operation of the original air interface is preserved. Many useful functions in the data security context are absent from ISO 15693. These include the following.

Passwords

The library data stored in the RFID tag's memory is not password-protected; therefore anyone with the capability of altering tag data will be able to do so.

Reader verification

The concept of authorised and unauthorised RFID reading devices is not found within ISO 15693. Again, anyone with the capability of altering tag data will be able to do so.

Physical item security

In libraries, physical Item security using the RFID tag is most commonly employed by setting one of two values in the Application Family Identifier (AFI) field contained within the tag's system memory area. The intended purpose of this AFI field is to indicate to an RFID reader which tags belong to the same application "family" as does the reader. For example, an RFID application tasked with scanning tagged aircraft baggage would be able, by means of the AFI, to discriminate between RFID tags on library items inside a suitcase and the suitcase itself, because the library items and the suitcase would be members of different application families. As the number of RFID tags in the community increases, the need for selective reading of tags becomes more important. Although not the original intent, the AFI may also be used as the basis for a security system as we will see.

The appropriate ISO registration authority has allocated an AFI value (C2) to denote circulating library items. A generic internal use code (07) also exists and may be used to denote library items on shelf. Together, the two can be used to construct a security system. Toggling between these two values during circulation processes allows the library's security system to determine whether the item should trigger an alarm or not. An item having the on-shelf code in its RFID tag's AFI field should not be leaving the library and the security system will alarm in this circumstance.

However, under the ISO 15693 standard, the AFI value is not protected by a password. Anyone with the capability of writing to a tag, and an understanding of this AFI security methodology (now in the public domain as part of ISO 28560) could turn off the item's security protection by simply changing the AFI value.

Locking data

One of the useful possibilities offered by ISO 15693 is to lock data. This could be system data (as in the case of the AFI) or it could be library data in the user memory such as the item identifier. However, the absence of password protection for this locking function means that it proves to be a two edged sword, as we will see. Anyone with the capability of writing to the tag can choose to lock the data on the tag.

Considering the vulnerabilities described above, what might be some of the attacks that could be mounted against the normal operation of the library RFID system? Several of these are considered in the following sections.

Broadly, attacks can be grouped into several (somewhat overlapping) categories as described below:

Denial of service

A denial of service attack is aimed at disrupting the use of a system or part of a system, to the extent that it can no longer, in practical terms, be employed by legitimate users. The attack may have no other aim except to cause frustration among users and staff. It is also important to note that for a denial of service attack to be effective, it is not always necessary to completely disable a system. As an example, consider an attack that simply locks the RFID tag's AFI value in on-shelf material. This will result in an alarm at the security gates irrespective of whether the item has been issued or not, because the security status of the tag can no longer be changed.

Using simplified numbers and logic for the purpose of illustrating a point, assume we have a busy branch library transacting 500,000 loans per year, open six days per week across a 50-week year, accounting for public holiday closures and similar. Let us further assume that the average user borrows five items. This translates to an average of 333 users per day with five items each. If one in twenty-five tagged items on the library shelves has its AFI security status locked, the alarm would be triggered on average by every fifth borrower, resulting in 67 alarms every day of the year. This would be a sufficient number of alarms for the security system to be turned off in an attempt to reduce the disturbance caused.

In this admittedly simplified example, targeting only 4% of the branch's collection constitutes an effective denial of service attack on the security infrastructure. A similar volume of items affected in other ways could cause self-service to be effectively unusable also. To rectify such an attack would involve the identification of every affected tag and then their removal and replacement.

Digital vandalism

This is essentially malicious activity, sometimes for no obvious purpose. A range of possibilities exists here, involving a smartphone app and a library RFID system:

- Erasing tags. The memory of the RFID tag could simply be overwritten.
- A combination of overwriting the tag's user memory and then locking it would ensure that not only is normal operation interrupted, but also that the tag must

be physically replaced to restore its function. Locked user memory cannot be unlocked.

- In a variation of the graffiti trend of “tagging” walls and other objects with spray paint cans, a specific signature could be written to the memory of RFID tags, using a smartphone as a kind of hacker’s ID, potentially displaying a message when the tag is examined. Apps are available that allow notes on the smartphone to be encrypted by means of a secret key stored on an ISO 15693 RFID tag. An interesting alternative in the “tagging” scenario would be to store encrypted messages on library RFID tags, the reading of which could only be accomplished by users sharing a secret key on their smartphones.

Item theft

Within most Australian libraries the RFID tag is tasked with managing item security as well as item identification, the manipulation of the tag’s AFI by a smartphone with a steal-my-library-book app would be quite simple. In the popular circulation context of self-service loans, a library user walking straight out with library material in hand is unremarkable and so this kind of theft might be difficult to detect.

The context also exists where item identifiers might be simply swapped. One very expensive and one very inexpensive item could be loaned by a user and, while on loan, the item IDs could be swapped. The inexpensive item masquerading as the expensive one could be returned and the expensive one claimed to be lost. The user therefore essentially gets to buy the expensive item at the inexpensive item’s price.

Evidence exists to indicate that there are already individuals equipped with smartphones who are taking an interest in library RFID tags. There are threads freely accessible on the Internet that chronicle the efforts of curious individuals as they progressively untangle the contents of library RFID tags and attempt to clone them.

Potential mitigation strategies

Encryption

One of the most common responses when speaking about the data security issues of library RFID systems relates to the possible use of data encryption. The ISO 15693 standard is silent on the topic of data encryption. This means that the information on the tag could be revealed by someone willing and able to read from the tag’s memory and then decode the information. The adoption of ISO 28560 as a data storage standard means that the encoding rules are in the public domain.

Of course, some (but not all) data could be encrypted before it was stored on the RFID tag, and then decrypted at the time the tag was read. Ignoring the processing overheads and interoperability consequences of such an approach, the major problem with encryption is that it addresses only the issue of keeping the RFID tag data unknown. Given that most if not all of the data within the memory of the RFID tag concerns the item to which it is physically attached, keeping this information secret does not in practice represent a major improvement, and could potentially cause more problems than it solves. For the purposes of this paper, the assumption

is made that the revealing of RFID tag item data through the use of smartphones does not, of itself, constitute a significant threat within the overall mix of vulnerabilities.

Easily realised and effective strategies that do not limit interoperability are limited under ISO 15693, for the reasons discussed previously. While a full discussion of all available options is not achievable within one conference paper, an overview can be provided. Should the threat from NFC-equipped smartphones be assessed as significant by an institution, mitigation strategies will be required to protect collections from item theft and to ensure the integrity of the RFID tag's user memory. Mitigation strategies should also not affect the tag's compliance with ISO 28560, the new interoperability standard for libraries.

Essentially the options for a library fall into two categories:

- Using standard ISO 15693 tag commands or features
- Using proprietary tag commands or features

These will be considered separately in the following sections.

Using standard ISO 15693 tag commands or features

These options rely on standardised commands and therefore are available to all libraries using High Frequency RFID tags and centre on memory locking of some type. It should be remembered that once locked, RFID tag memory may not be unlocked, and so careful thought is needed before implementing a locking strategy.

Theft prevention

Unfortunately, simply locking the AFI to prevent an antagonist from changing it is not a solution inasmuch as it would also prevent the library from using the AFI as a security system. In practice, the only effective course of action open is to abandon the AFI security system and implement a separate security infrastructure for library items. This is not an attractive strategy for many libraries that have retired such systems following the migration to RFID.

User memory protection

In this area, ISO 15693 has options that are more useful. One such option would be to lock the user memory of the tag, which would essentially prevent an antagonist from changing or erasing the library data. In the vast majority of Australian RFID implementations, the user data is not locked and is therefore vulnerable. Ideally, suppliers would need to design an appropriate methodology for efficient memory locking, perhaps as a special activity with the hand-held device, combined with an automatic function at the point of item returns or as part of a migration to ISO 28560. Locking of tag data for new items could be easily accomplished, as it is a standard function of ISO 28560.

ISO 28560 allows for selective locking of data elements. This is a very useful feature. It would permit a library to lock all of their ISO 28560 encoded data elements (perhaps with the exception of the content parameter), which would prevent any service disruption from acts of digital vandalism. By leaving the unused portion of the

tag's memory unlocked, additional data elements could still be added in the future while remaining compliant with the standard.

Using proprietary tag commands or features

We have mentioned the limitations of ISO 15693 tags previously. Some RFID chip manufacturers have sought to rectify the situation by adding proprietary commands or functions to their ISO 15693 tags. These commands and functions act as a sort of extension to the basic ISO 15693 command set.

The most common of these enhanced functionality chips for RFID tags are supplied by NXP Semiconductors, one of the world's largest suppliers of RFID chips. In Australia, the most common NXP chip having useful functionality in the smartphone threat context is the NXP SLIX chip. At the time of writing, the major RFID suppliers in Australia offer, as standard, RFID tags having this chip type. The SLIX chip offers two useful but non-standardised features (plus a fifty-year data retention life – not germane to the smartphone discussion but potentially very useful to many libraries):

- Password protection for the changing of RFID tag AFI values
- A separate and password protected Electronic Article Surveillance (EAS) function for item security

For libraries that already have the NXP SLIX chip in their RFID tags (or who choose this chip for new stock) and have the appropriate reader hardware, a number of additional mitigation strategies are made available. Of course, to utilise these options is to base a strategy on a specific chip manufacturer and non-standardised functionality, but considering the penetration of NXP hardware in the library sector, it must be included here as part of the discussion.

Theft prevention

Using SLIX equipped tags, a concerned library could implement a strategy that:

- Locks the AFI value on the tag at the value for circulating library material
- Implements the password protected EAS function for local item security

This would effectively preserve the RFID tag-based item security infrastructure. Of course, the library's RFID supplier would be required to support the SLIX additional functionality but hardware support at least may already be present. Should the library decide to leave the AFI unlocked, other ISO 28560 libraries could use the AFI for security when the item was under their control: during an inter library loan, for example. As the chip's EAS security function has been set out of scope for ISO 28560, the compliance of the RFID tag with the standard is not compromised.

A library could also choose to employ the password-protected AFI value of the SLIX chip; however, here the compliance of such a scheme with ISO 28560 is open to challenge. There is also the issue of password management in contexts where collaborative arrangements exist for resource sharing. The larger the password domain becomes, the more difficult it is to maintain secrecy.

User memory protection

As the SLIX chip is ISO 15693 compliant, the same memory locking function available to all standardised tags could be used to protect the user memory.

Conclusion

It has always been possible for an antagonist to procure a standard High Frequency RFID reader, which might then be used in a malicious way within the library. However, such an attack would have only local consequences. The proliferation of NFC-capable smartphones and ready access to apps has changed the threat dynamic. The situation now exists where practically every library will have numerous members possessing hardware capable of mounting an attack on the RFID system. Apps having the capability to overwrite library RFID tags are also freely available. The consequences of one individual developing a specific steal-my-library-book app (or a trash-my-library app) may be felt internationally and within days of the app's release.

Of course, the business of threat assessment must take place at the level of the individual institution and will take into account a range of factors. What we can reasonably say, however, is that whatever risk level existed in the past, it has now changed and perhaps a new evaluation is required.

Library managers having concerns about the negative potential of NFC-equipped smartphones may wish to consider mitigation strategies, some of which have been briefly described in this paper, if not for all existing stock, then perhaps as an additional step in new item processing.

References

Balaban, D., 2013, *NFC Smartphone chip shipments in 2012 surge past projections*, NFC Times, retrieved 12 October 2013, from http://nfctimes.com/news/nfc-smartphone-chip-shipments-2012-surge-past-projections

Finkenzeller, K., (2010) *RFID Handbook - Fundamentals and applications in contactless smart cards and identification*, Third edition, Wiley, p. 57

Infineon, 2013, *Security on NFC-Enabled platforms*, Infineon.com, p. 4, retrieved 12 October 2013 from http://www.infineon.com/export/sites/default/media/Applications/ChipCards/NFC_Whitepaper_09.2013.pdf

Lykke-Oleson, A., Nielsen, J., 2007, *BibPhone – Adding Sound to the Children's Library*, retrieved 2 December 2013 from http://www.interactivespaces.net/data/uploads/papers/19.pdf

Petrovan, B., 2013, *Galaxy S3 sold 50 million units, demand for Galaxy S4 deemed "explosive"*, Android Authority, retrieved 12 October 2013, from http://www.androidauthority.com/galaxy-s4-demand-galaxy-s3-sales-197892/

Ranger, S., 2013, *Don't ditch your wallet just yet*, ZDNet, retrieved 12 October 2013, from http://www.zdnet.com/smartphone-payments-via-nfc-dont-ditch-your-wallet-just-yet-7000011846/

Vedat, C., 2012 *Near Field Communication – From Theory to Practice*, Wiley, pp. 11-13