

Tag, you're it - NFC in a home environment

Veli-Jussi Raitila
Helsinki University of Technology
vjr@iki.fi

Abstract

This paper envisions the application of Near Field Communication (NFC) in a home environment. Several NFC solutions are currently available in the logistics industry relying on Radio Frequency Identification (RFID) in addition to others being adopted for personal mobile interaction. We will demonstrate what separates a domestic setting from the aforementioned ones as well as the implications of those differences. Once the distinction has been made, we will present a comprehensive set of ways to exploit this technology in a smart home.

KEYWORDS: nfc, near field communication, smart home, pervasive computing

1 Introduction

1.1 NFC in brief

Near Field Communication (NFC for short) is a standards-based (ISO, ECMA, ETSI) short-range wireless technology that utilises magnetic field induction within the unlicensed frequency band of 13.56 MHz. It is not regarded as a competing solution to other wireless technologies such as Bluetooth or Wi-Fi, but rather a complementing one. Because of the relatively short operating distance of a few centimeters and low transfer rates (106, 212 or 424 kbps) NFC is often used to configure secondary communication protocols to handle the main bulk of traffic. The process is initiated by bringing the objects close enough to virtually touch each other. Other applications include RFID (acting as a tag and/or a reader) and smart card emulation. An NFC-enabled device, typically a mobile phone, functions in either passive or active mode i.e. by drawing power from and modulating an external field or by generating one of its own. Near Field Communication is being promoted by The NFC Forum and its over 100 members including NXP Semiconductors, Sony and Nokia as well as several telcos and mobile network operators from the GSM Association.

1.2 NFC applications and RFID

Today the concepts behind NFC technology can be seen in a wide range of applications. For example, passive RFID tags and their appropriate readers are being used as means of tracking goods along the supply chain from a manufacturer, through warehouses and distribution centers all the way up to a retailer. Some governments issue personal documents such

as passports that can be read at a distance. Both of these approaches have led to a flurry of security and privacy concerns as well as attempts to solve them [9]. Majority of the issues arise from the fact that the infrastructure that surrounds these solutions is not controlled by the carrier of the tag, but rather a separate entity whose actions need to be trusted. Another threat stems from the inherent wireless nature of communication used in those systems.

Some of the recent, and probably the most common NFC applications (Fig. 1) such as electronic payment and ticketing by using a mobile phone, turn the table around. The user is now (at least partially) in charge of the interaction, activating functions associated with tags or other NFC-enabled devices around him. Although that level of control is often used as a marketing slogan, it is true at least to a point. The operating distances of such devices are also significantly shorter, mitigating the risk of eavesdropping. That risk is completely negated when a secure channel is established after device pairing [6]. Security issues aside, the technology seems promising and might very well gain the acceptance of the masses. It brings the natural "rituals of touching [5]" back into human behavior with the help of an unlikely medium of human computer interaction.

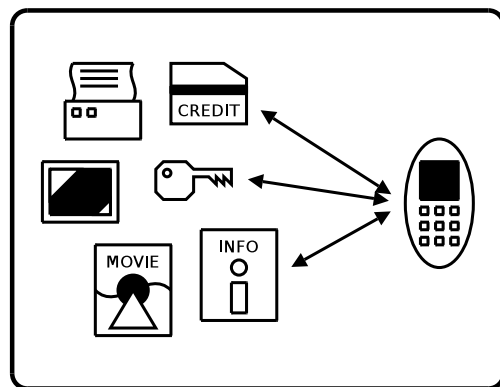


Figure 1: Common NFC applications

Utilising Near Field Communication in a home environment takes this distinction one step further however - the person is in complete control of both the infrastructure and the devices functioning in it. This enables a whole new level of automation and personalisation of everyday household tasks and activities. Ultimately a network of context- and location-aware nodes can be created, where the user does not simply identify the device he is using or the action he wants to take, but the device itself identifies the user as well as other objects around it and acts accordingly. In the following chapters we

will first paint a crude picture what widespread adoption of RFID-technology would mean in a home environment and delve into the steps that need to be taken in order to reach that goal. It is clear that several obstacles need to be overcome, most of them being not so much as technical as they are behavioral. After that we will briefly go through some of the security and privacy issues related to the use of NFC tags and NFC-aware home appliances. Finally, a set of example applications are given, grouped into three conceptual categories.

2 User acceptance and usability

Recent studies show that while the general public might be eager to embrace new technologies that employ NFC and/or contain RFID tags, their knowledge in the area is limited and lacks the appropriate mental models [3]. This poses a serious usability problem. The wider audience need to become familiar with the concepts and to identify the benefits within before they invite novelty gadgets in their homes. Furthermore, the users need to recognise the items that implement the functionality in question. That can be achieved by providing visible cues, marking the objects with clear graphical symbols indicating that the device has NFC properties [2].

In spite of a great deal of research that has been done in trying to make RFID tags as affordable as possible, it is still not cost-effective to put them on each and every item. That is not to say that it will not be the case some day. Until that happens, however, it is highly unlikely that the consumer will pay anything extra especially if the additional value is not clear to them right from the start. The same applies to more complex NFC functions as well, being integrated into mobile phones or otherwise. As always in the area of marketing, new consumer needs are difficult if not impossible to create and all efforts should be aimed in finding the existing ones.

There is no denying that a mobile phone is by far the most common ubiquitous computing platform available to the general public. Therefore, it is only reasonable that all the current Near Field Communication applications rely on it. Most of the advertised features are also mobile in nature, so it is the obvious choice in performing those activities. However, it can be argued that a mobile phone has its limits as a universal interaction device [16]. This applies particularly to a home environment. Most of the tasks involving household appliances are pervasive in nature and using a device originally designed for something completely different (mainly placing calls and talking) may introduce unnecessary steps to the process and irritate the user. Besides, we really cannot expect a person to carry his mobile phone around the house at all times. Another concern with multi-purpose devices as a whole is the risk of putting "all the eggs in one basket". What happens if the phone is stolen?

Although a mobile phone has its limitations, it can justifiably be used in some special circumstances such as near the exit area or in the close proximity of a house (yard, garage etc.). We will go through some of the examples in the following chapters in more detail, but in general it is safe to assume that the user will be holding his mobile upon entering or leaving the premises. The most obvious choice would be to use an NFC-enabled phone as means to provide access

control i.e. use it as a key, but there are others, perhaps more suited alternatives as we will soon see.

3 Home and the Internet of Things

If we are willing to accept that RFID tags are becoming more and more commonplace and NFC applications emerge in the mobile market, it is only a matter of time when we will find this technology in our homes. But as we have pointed out earlier, a phone is not necessarily the best all-round NFC device for this type of environment. Instead, we would like to claim, that a more viable option would be to *embed NFC into existing household items*. Infrastructure-wise that would ultimately imply things like smart furniture, smart surfaces (walls, floor panels, tables) or even smart spaces [8, 12, 19]. A smart home is most probably a networked one as well, which would provide means of communication between the different artifacts or access into a back-end system for more processing power and practically limitless data storage.

Why stop there? As tags become smaller and smaller they can be inserted nearly anywhere. A taste of what is to come might be the latest generation of RFID chips from Hitachi, unveiled in February 2007, measuring only 0.05 x 0.05 mm in size. Tags could be woven into the fabric of our clothing, surgically inserted under our skin or even ingested [18, 14]. Active components follow the same path of miniaturisation and research has been made on wearable tag readers [17] among others. When devices such as these are located so close to the human body or even inside it, alternative transmission mediums have been considered as well. A technology called BodyNFC demonstrates how "electronic devices on and near the human body can exchange digital information by capacitively coupling picoamp currents through the body [22]". Many of these technologies mentioned are exploitable in a home environment.

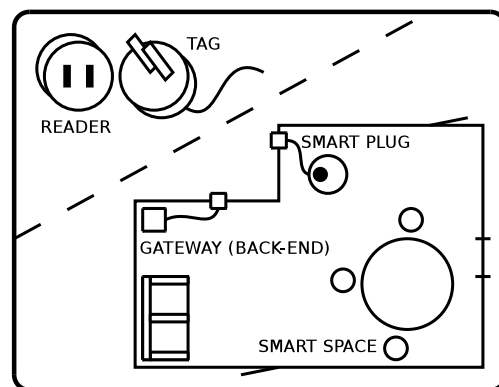


Figure 2: A smart plug in a smart space

First household solutions will without a doubt, assuming NFC ever truly catches on, be local in nature. What this means is that only a few items participate in any given activity and no complex infrastructure is required. It is also equally probable that in this type of a scenario the user has a crucial role in everything that happens. Yet at some point one can imagine an Internet of Things, where numerous inanimate objects have been given identities and a location they

inhabit in a smart space. The objects "sense" each other as well as the context they are in, allowing varying levels of autonomy (e.g. the stove acts as a smart surface and by seeing olive oil, onions, garlic and tomatoes, deduces the person must be making tomato sauce). If we extend the notion of smart spaces into a larger scale, the whole house for example, these collaborating artifacts might be implemented by using a concept of *smart plugs* [4] - implying an automatic configuration, monitoring and operation of household devices as soon as they are physically connected to a back-end system via network cabling (Fig. 2). In case of simpler devices, such as lamps, radiators and AC, the power grid could be used instead.

The role of NFC in an Internet of Things could be either in binding objects together or in enabling a controlling entity (a person) to manipulate them and administer the system, possibly both. There has to be a degree of self-governance however, because in a home environment one can not simply call tech support if something unexpected happens. Streitz et al. [19] suggest a division of smart artifacts into system-oriented (importunate smartness, automation) and people-oriented (empowering smartness, user guidance). The end result depends on the application domain and will likely be something in between. There are several studies available related to enabling smart spaces with help of the Open Services Gateway initiative (OSGi) [12, 4], automatic service composition [21] and making adaptive context-aware applications [7].

4 Security and privacy

Almost every technology that exploits RFID also raises questions about its impact on security and privacy. Some of those concerns are well founded and some are not. It is worth noticing that using NFC in a domestic setting differs from most of the earliest scenarios in more ways than one. To begin with, a home should be a relatively isolated environment. If that is not the case, deficiencies in the physical security are the ones that need to be taken care of first.

Secondly, and related to the previous argument, ranges involving NFC communication are relatively short. Nevertheless, one can not claim that it is completely immune to eavesdropping. It is not. The situation can be significantly improved, however, by resorting to passive mode whenever possible. The protocol is also by its very nature, resistant to man-in-the-middle attacks and therefore an ideal setup would be to use NFC merely in the key exchange phase and to establish a secure connection between two devices [6]. The exchange can be done without authentication and a separate channel with the help of a higher speed protocol, such as Bluetooth is also capable of compensating for the low transfer rates of the NFC.

Thirdly, as RFID tags are known to contain only relatively small amounts of information, they are not an interesting target for attackers. The main bulk of information is often held in a back-end system. Keeping that secure should be of utmost importance. A smart home would most likely be controlled by some type of a middleware platform and attacking the infrastructure (Fig. 3) could be tempting. That is especially true if it is connected to the Internet in a way or an-

other. The risks become higher concerning a single device as its capabilities increase and a mobile phone is a very capable device indeed. On a related note Stefano Puglia et al. [15] classifies RFID-based architectures as being back-end based (BEA), full mobile device based (FDMA) or partial mobile device based (PMDA). The choice of a particular architecture also affects the way security has to be designed.

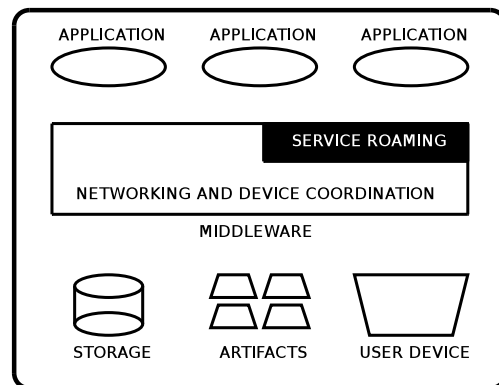


Figure 3: Example architecture: devices, middleware and applications

There are several active steps that can be taken to increase security at implementation level, keeping in mind that every choice may decrease the usability of the system. If, for example, user authentication is required, a passcode prompt could be shown in order to verify a certain NFC gesture. In extreme cases that passcode could be one-time only and/or combined with biometric sensors to provide extra assertion. If used to implement access control the overall infrastructure should be resistant to for example replay attacks and handle situations where the device is lost or stolen. Some could be allowed limited or temporary access and others blacklisted indefinitely. Using NFC for access control is justifiable in environments with restricted areas and a large amount of people coming and going. Such places would include workplaces, hotels and perhaps rental apartments. Indeed, research has been made on how to provide admittance services through SMS-messages and NFC-enabled mobile phones [13]. Why it might not be applicable to homes in general, is that there would have to be a backup system in case the main one does not work.

If we expand our analysis into smart homes mentioned in the previous chapter, using NFC might in some cases actually increase security or at least increase the usability aspects of it. When homes fill up with networked devices, setting them up might be a pain for a non-technical person. Already today there are numerous (unintentionally) open wireless access points around the globe and that merely proves our point. NFC could be used to securely automate the installation of these networks and the peers functioning within them [1].

Consequently, it is not that RFID as a technology is somehow inherently insecure or infringes upon our privacy. In the end what matters is how we use that technology. It is also worth considering whether the home applications and information transferred within them is all really worth protecting so vigorously. As far as real life is concerned, much of it is

not. And even if some of it were, the misuse of touch-based NFC devices would be hard to accomplish unnoticed. It would be the digital equivalent of stalking, peeking through windows, general mischief or ultimately breaking into people's homes and we have laws to protect us against that sort of behavior. This leaves us with the threat from within. Are we able to trust our own family members? If not, there is no technology that will help us remedy that. So at least to some extent, the risks are already there and using RFID does not add anything to the equation. We have to emphasise though, that we are talking about home applications. The situation is drastically altered when we go out the door.

5 Example applications

We have divided this section into three separate (but not mutually exclusive) categories. Short descriptions are given on several example applications in which the technology could be used. Temporal viewpoint analyses what type of NFC-enabled solutions would benefit the user the most at a given moment in time. Spatial viewpoint highlights applications tied to a specific room or space and demographical viewpoint takes the age of the user into account. This categorisation is in no way exhaustive and several others could be added.

5.1 Temporal viewpoint

In most of the following cases (both at night as well in the morning) the user would not have to be automatically identified, but rather he would use an NFC device to administer the system. Appropriate control panels could be scattered around the house and accessed on demand. In the situations where the user does need to be recognised, it could be done by scanning for worn or implanted tags.

- Morning/Evening
A *smart alarm clock* would set the alarms according to the persons sleeping nearby whereas a *smart bed* would control its hardness, shape and tilt as chosen by the user who lays on it. Some of the morning routines could be personalised and automated (boiler startup, turn on floor heating, make coffee etc.)
- Night
During the night the role of automation is accentuated. Things like air-conditioning and/or heating could be automatically adjusted on the basis of presence information or personal preferences.

5.2 Spatial viewpoint

- Study
A "traditional" application would be a *smart printer*, which upon contact, prints images or documents offered to it from mobile phones, digital cameras etc. The same idea is applied to transferring pictures to a *smart picture frame*. Perhaps the frighteningly common USB memory sticks might be replaced by their NFC-empowered equivalents, providing additional security to personal data storage in the process. What ties all these solutions together is the method of using NFC to initiate

the transaction and let a higher speed protocol take over from there.

- Hall
Gate reminder is a type of a bulletin board that "reminds users of the objects they forget to carry and the messages they need to know when leaving home [10]". The user might be notified of inadequate clothing or that their umbrella is still in the closet while it is pouring outside. A useful implementation would require tags on key items as well as means of identifying the user. Since a hall can be considered as an entry/exit area, use of a mobile phone can be justified. Consequently, a simpler scheme could be applied to a case when the user is about to forget his phone.
- Kitchen
Presuming that all groceries had RFID tags on them, a *smart refrigerator* would keep track of the items in it and their expiration dates. It could also provide recipes that contain the ingredients taken out from it and give dietary advice. The refrigerator would in this scenario function as a mere tag reader, but it should have access to a back-end system. A *smart microwave oven* on the other hand could recognise the food item about to be inserted in it and set the timer along with adequate power settings for heating up the meal. It should be noted, that the package containing the TV dinner should have clear instructions on how to remove the tag and the operation should be easily accomplished to avoid damaging the oven.
- Living room
A *smart media center* could recognize its user and configure his favorite channels into the TV, load up playlists into the media player and choose a preconfigured keymap into a universal remote. Maybe the remote itself would be NFC-enabled. How the user would be identified ranges from implanted/ingested tags to wearable ones, all the way up to BodyNFC. Music and movies could also be transferred from external media to the center's hard drive by touch. Naturally, this would require the media (or any other storage device) to be NFC-capable. Since the storage space on the tags is limited, the information transmitted could be narrowed down to metadata only (movie cast, artists, dates etc). Taken this even a step further, the media might not contain the actual content at all, but rather a set of credentials to allow downloading movies or other articles through a back-end system.
- Laundry/Utility room
If clothes were embedded with RFID tags, a *smart washing machine* could choose the appropriate program for them, select the correct temperature and prevent from starting the cycle if colored items were mixed with white ones. Challenges in this scenario include how to make the tags durable enough to withstand constant wear and tear and at the same time make them removable if wanted. On the other hand, basic information such as material, color and preferred temperature requires very little storage space. Therefore a set of tags

might be used, where the part that contains privacy infringing information could be removed and the rest not as easily. Analogously, a *smart steam iron* could be designed.

- Garage
In a *smart car* NFC-enabled device could be applied to a wide array of situations including access control, personalised seat, mirror and driving style settings. Driver's health could also be monitored in order to prevent falling asleep at the wheel or to warn of acute medical conditions. In the latter case, a combination of medical sensors and NFC to transmit the data could be used.

5.3 Demographical viewpoint

- Children
Most appropriate NFC solutions for children would naturally involve games and toys. *Smart lego* blocks could change color or emit sounds when combined with each other. Example games might be for example variations of "Tag", such as "Tagaboo [11]".
- Adults
Adults with small children would appreciate solutions which promote child safety. Tracking tags could be stitched into toddlers' clothing and potentially dangerous household equipment such as ovens might be fitted with proximity sensors. Authentication would be required in operating a lawnmower or opening drawers with medicine, detergents or sharp objects.
- Elderly
NFC can be used in various health care applications, such as off-line monitoring of heart rates, weight, glucose and blood pressure [20]. A *smart medicine cabinet* could provide information about its contents as well as remind that prescribed drugs are taken regularly. Other application areas would be in automating everyday household activities, which applies also to disabled and handicapped persons.

6 Conclusion

Near Field Communication is an interesting technology. It allows people to perform actions, manipulate objects and gain more information about them by a simple gesture of touching. In the long run it might also enable a personalisation and automation of every day household activities along with the Internet of Things. Until the technology becomes ubiquitous in homes, however, the general public need first to familiarise itself with it. That might happen with the help of the applications designed for mobile phones, such as electronic payment, ticketing and information-on-the-move. Using a mobile phone at home, on the other hand, is not always reasonable and a better option would be to integrate NFC chips into existing household items. Many of the presented solutions are already technically feasible and security is almost a non-issue (isolated environment, sound implementations). Finally, as far as the widespread adoption of

RFID-enabled devices goes, the greatest challenge might be to convince the consumers of their usefulness.

References

- [1] Z. Antoniou and D. Kalofonos. NFC-based mobile middleware for intuitive user interaction with security in smart homes. *submitted for review*, 2006.
- [2] T. Arnall. A graphic language for touch-based interactions. *Mobile Interaction with the Real World (MIRW 2006) Workshop, Espoo, Finland*, 2006.
- [3] S. Belt, G. D., and M. K. User Perceptions on Mobile Interaction with Visual and RFID Tags. *Mobile Interaction with the Real World (MIRW 2006) Workshop, Espoo, Finland*, 2006.
- [4] H. Elzabadani, A. Helal, B. Abdulrazak, and E. Jansen. Self-sensing spaces: smart plugs for smart environments. *3rd Intl. Conf. on Smart homes and Health Telemetrics, July*, 2005.
- [5] A. Galloway. The rituals of touching. *Touch, research project blog*, 2006.
- [6] E. Haselsteiner and K. Breituß. Security in Near Field Communication (NFC) - Strengths and Weaknesses. *Workshop on RFID Security, Graz*, 2006.
- [7] M. Huebscher and J. McCann. Adaptive middleware for context-aware applications in smart-homes. *Proceedings of the 2nd workshop on Middleware for pervasive and ad-hoc computing*, pages 111–116, 2004.
- [8] M. Ito, A. Iwaya, M. Saito, K. Nakanishi, K. Matsumiya, J. Nakazawa, N. Nishio, K. Takashio, and H. Tokuda. Smart furniture: improvising ubiquitous hot-spot environment. pages 248–253, May 2003.
- [9] A. Juels. RFID security and privacy: a research survey. *Selected Areas in Communications, IEEE Journal on*, 24(2):381–394, 2006.
- [10] S. Kim, M. Kim, S. Park, Y. Jin, and W. Choi. Gate reminder: a design case of a smart reminder. *Proceedings of the 2004 conference on Designing interactive systems: processes, practices, methods, and techniques*, pages 81–90, 2004.
- [11] M. Konkel, V. Leung, B. Ullmer, and C. Hu. Tagaboo: a collaborative children's game based upon wearable RFID technology. *Personal and Ubiquitous Computing*, 8(5):382–384, 2004.
- [12] C. Lee, D. Nordstedt, and S. Helal. Enabling smart spaces with OSGi. *Pervasive Computing, IEEE CS and IEEE ComSoc*, 2(3):89–94, 2003.
- [13] J. Noll, J. C. L. Calvet, and K. Myksvoll. Admittance services through mobile phone short messages. pages 77–77, July 2006.

- [14] K. Okada, T. Yamada, T. Uezono, K. Masu, A. Oki, and Y. Horiike. Near field communication chip using PIM for bio MEMS sensors. pages 440–441, Aug. 2004.
- [15] S. Puglia and A. Vitaletti. Alternative RFID based Architectures for Mobile HCI with Physical Objects. *Mobile Interaction with the Real World (MIRW 2006) Workshop, Espoo, Finland, 2006*.
- [16] C. Roduner. The Mobile Phone as a Universal Interaction Device - Are There Limits? *Mobile Interaction with the Real World (MIRW 2006) Workshop, Espoo, Finland, 2006*.
- [17] A. Schmidt, H. Gellersen, and C. Merz. Enabling Implicit Human Computer Interaction - A Wearable RFID-Tag Reader. *Proceedings of the International Symposium on Wearable Computers, ISWC2000*, pages 193–194, 2000.
- [18] R. N. Simons, F. A. Miranda, J. D. Wilson, and R. E. Simons. Wearable wireless telemetry system for implantable bio-MEMS sensors. pages 6245–6248, Aug. 2006.
- [19] N. Streitz, C. Rocker, T. Prante, D. Van Alphen, R. Stenzel, and C. Magerkurth. Designing Smart Artifacts for Smart Environments. *Computer*, 38(3):41–49, 2005.
- [20] E. Strommer, J. Kaartinen, P. J., Y. oja A., and I. Korhonen. Application of near field communication for health monitoring in daily life. *Proceedings of the 28th IEEE EMBS Annual International Conference. New York City*, pages 3246–3249, 2006.
- [21] P. Wisner. Automatic Composition in Service Browsing Environments. *Mobile Interaction with the Real World (MIRW 2006) Workshop, Espoo, Finland, 2006*.
- [22] T. Zimmerman. Personal Area Networks: Near-field intrabody communication. *IBM Systems Journal*, 1996.