Near-field communications

Jon Titus, Technical Contributor

Prepare to take NFC beyond the obvious mobile-payment apps.

Near-field communications, which arose from earlier RFID applications, have gained in popularity as manufacturers added NFC capabilities to smartphones and tablet computers and as merchants have installed NFC payment devices. So instead of carrying a wallet full of credit and debit cards, consumers can use their smartphones as a mobile-payment "account" that uses the Google Wallet app or the ISIS Mobile Wallet. Customers simply start their payment application and place their smartphone within a few centimeters of a point-of-sale terminal to complete a "contact-less" transaction. No card to swipe, no chance a restaurant server will "skim" card information, and no photo ID to present. According to Google, over 140,000 merchants accept Google Wallet payments.

Microsoft Windows 8 software, Windows Phone 8, and Surface hardware will include NFC capabilities, too. Microsoft already has application programming interfaces (APIs) for a PeerFinder and ProximityDevice class, so if you're an app developer you can jump into NFC and start to use it as you wish.

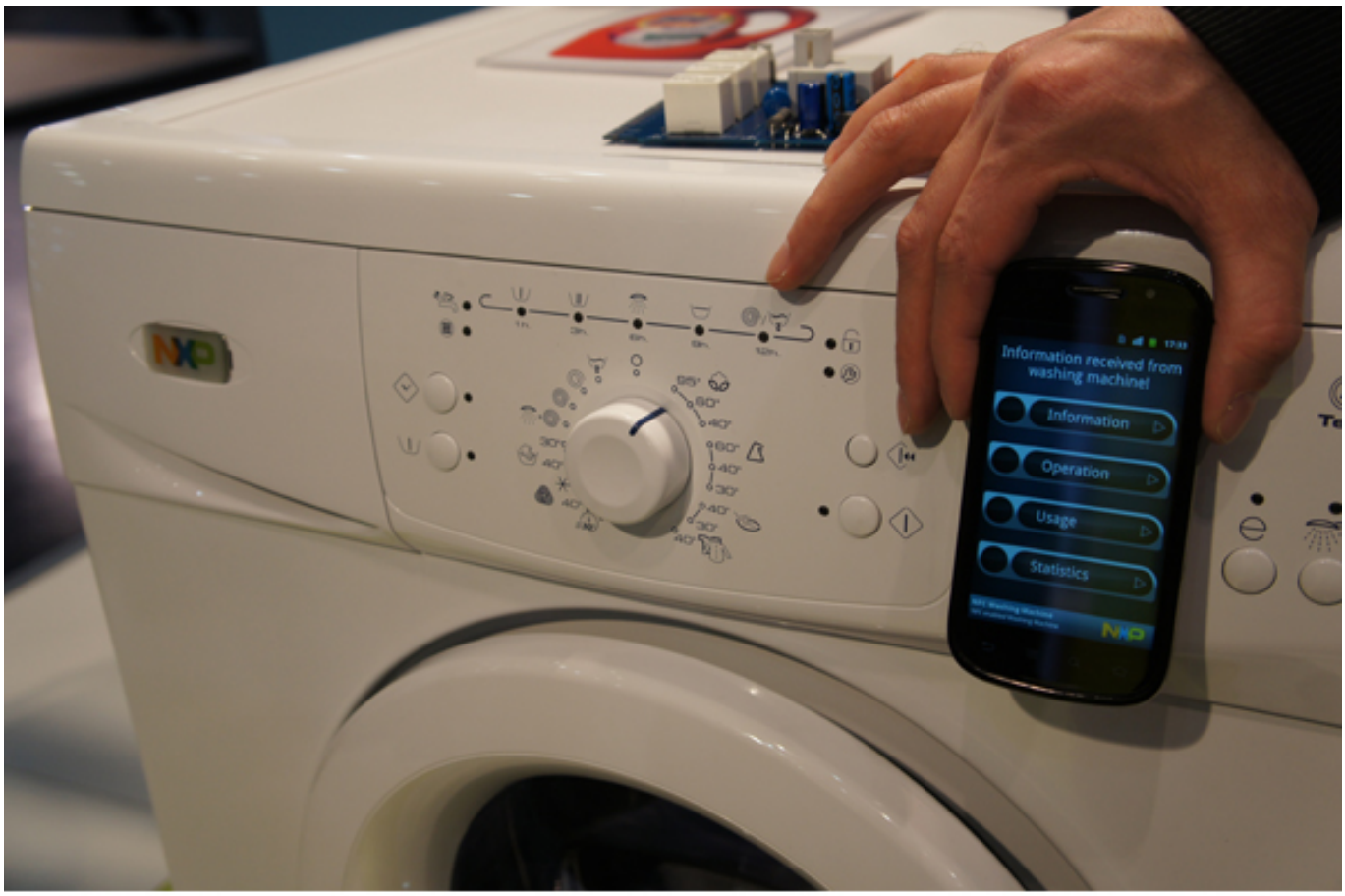

Figure 1. A technician can use an NFC-capable phone to gather diagnostic information from a smart washing machine. The phone also could upgrade firmware and launch an app that communicates with the manufacturer's service center. Courtesy of NXP.

While NFC contactless-payment apps dominate interest now, NFC devices will facilitate interesting uses unrelated to payments. And a choice of NFC chips from companies such as Broadcom, STMicroelectronics, Atmel, and NXP gives engineers and product designers many options to investigate.

"People will find NFC useful when they must 'pair' devices," explained Serge Fruhauf, senior technical marketing manager for secure micro and embedded security at STMicroelectronics. "Suppose you have a laptop and a Bluetooth docking station and mouse. To link these devices, you go through menus to configure them, and it becomes a chore. If you have NFC in the laptop and an NFC tag in the docking station and mouse, you can simply touch these devices to the laptop to associate them with it. No more menus and settings. You use NFC to make user experiences better and less complicated."

"I have a video taken with my mobile phone, and I want to show people, but not on the phone's small screen," said Mohamed Awad, associate product line director for mobile and wireless at Broadcom. "I touch the phone to the TV set and then transfer the video data via WiFi. When I do that, though, people think I transferred a big file over the NFC link. That link only indicated to the TV I have a phone with a video to play. The TV sets up the WiFi link to get the video file."

NFC can do more than identify devices, because specifications provide for a data rate as high as 424 kbits/sec and active-to-active device (peer-to-peer) or active-to-

passive device communications.

"You can could put a tag on a poster for a concert, for example, or put tags near products in stores to offer discounts," continued Fruhauf. "You can learn about the concert, get a link, and so on. You just get a small amount of information."

When people think about wireless communications, security comes to mind. "You have security inherent in the wireless link," said Awad. "Consumers might think hackers can easily get the NFC information, and the NFC industry must overcome this concern. In reality, NFC communications use a magnetic field, and its intensity drops off quickly. The NFC standards specify a maximum 10-cm separation between devices, but in practice, NFC devices need a separation of no more than about 4 cm. So to read data from an NFC device across a room would take a lot of power. It's not realistic to even try it." (See: "What's a Near Field?")

"The NFC Forum specifications do not cover secure communication," said Fruhauf. "The secure applications are loaded in a 'secure element,' that comprises a secure microcontroller, or a universal integrated circuit card [UICC] with Java and an operating system that connects to an NFC controller."

According to Gemalto, an electronic-security company, a UICC checks to ensure the right person has access to communications and applications, and it securely stores personal information. The UICC also will store algorithms and certificates that make it extremely difficult for another party to access your data and communications. If you use an NFC connection to pay for a plane ticket, for example, the payment application should access only payment information and should not interact with the actual plane-ticketing application or information.

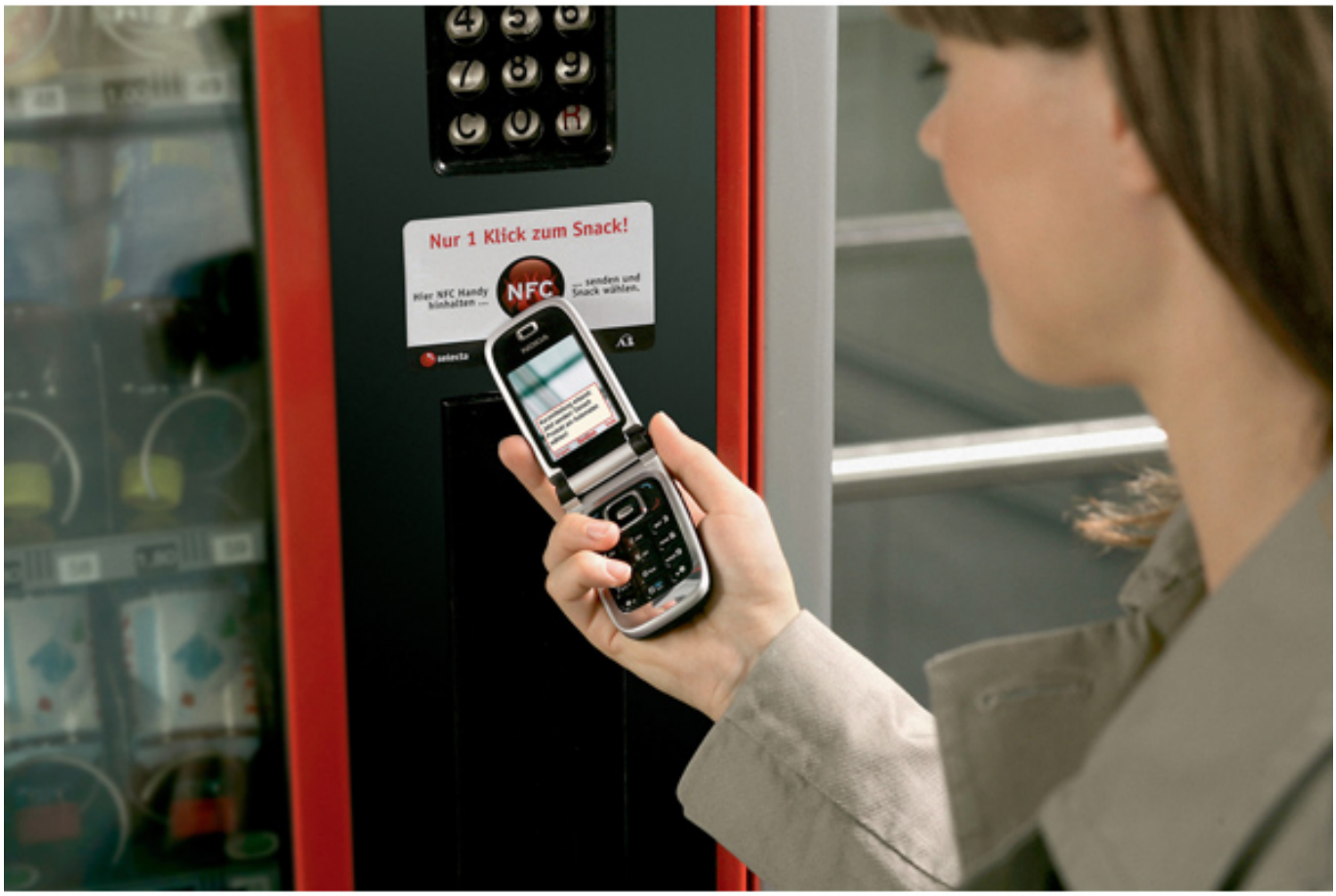

Figure 2. In Germany a snack from a vending machine might need just one click on a smart phone with NFC capabilities and a payment app.

The Toulouse-Blagnac airport in France has started a trial run for 50 frequent fliers who will use the NFC capability of their BlackBerry phones to access a car park, a premium-access zone for departures, and a private-lounge area. The airport aims to have broader NFC use in a year or two to let smart-phone owners board flights and pay for goods (Ref. 1).

I can envision use of NFC in a local coffee shop to make ordering easier. My order doesn't vary, so I could set up a smart-phone app to transmit my order to the servers as soon as I enter the store. That connection would save time and reduce confusion during rush hour.

What's a near field?

Maxwell's equations describe a near field as one close to an electromagnetic source and dominated by electric and magnetic components. So near-field communications rely on close proximity--usually one wavelength--to a transmitter. NFC communications use a 13.56 MHz frequency, so the near field extends to about 22 meters. That might seem like a long distance that could let hackers pick up NFC-transaction information. But the magnetic field from a current loop decreases with the inverse cube of the distance. If you have a 1G field at 1 cm from the NFC antenna loop and move to 10 cm, you then have a field of 1.0×10^{-3} G. The NFC standards specify a maximum 10-cm separation between devices, but in practice, NFC devices usually need a smaller separation: 0 to 4 cm.

NFC standards

ISO/IEC 14443: Identification cards--Contactless integrated circuit cards--Proximity cards (four parts)

ISO/IEC 15693: Identification cards--Contactless integrated circuit cards--Vicinity cards (three parts)

ISO/IEC 18092: Near Field Communication--Interface and Protocol, Part 1 (see also ECMA 340)

ISO/IEC 21481: Near Field Communication--Interface and Protocol, Part 2 (See also ECMA 352)
==========

Reference

1. Engadget: http://www.engadget.com/2012/05/24/toulouse-blagnac-airport-field-test-nfc/ [1]

For further reading

Near Field Communication (NFC) Controller, PN532/C1, NXP. http://www.nxp.com/documents/short_data_sheet/PN532_SDS.pdf [2].

Minihold, Roland, "Near Field Communication (NFC) Technology and Measurements," 1MA182, Rohde & Schwarz, 2012. http://www2.rohde-schwarz.com/en/service_and_support/Downloads/Application_Notes/?downid=7019 [3].

"Mobile NFC Technical Guidelines," http://serving.webgen.gsm.org/5926DA9A-2DD6-48E7-BAD4-50D4CD3AF30A/assets/gsmanfc2wp.pdf [4].

"NFC Technology," http://www.radio-electronics.com/info/wireless/nfc/nfc-near-field-communications-technology.php [5].

"NFC UICC Requirement Specification," Version 2.0, November 2011, includes a list of standard technical specifications. http://www.gsma.com/mobilenfc/wp-content/uploads/2012/03/gsmanfcuiccrequirementsspecificationversion20.pdf [6].

Links:
[1] http://www.engadget.com/2012/05/24/toulouse-blagnac-airport-field-test-nfc/

[2] http://www.nxp.com/documents/short_data_sheet/PN532_SDS.pdf
[3] http://www2.rohde-schwarz.com/en/service_and_support/Downloads/Application_Notes/?downid=7019
[4] http://serving.webgen.gsm.org/5926DA9A-2DD6-48E7-BAD4-50D4CD3AF30A/assets/gsmanfc2wp.pdf
[5] http://www.radio-electronics.com/info/wireless/nfc/nfc-near-field-communications-technology.php
[6] http://www.gsma.com/mobilenfc/wp-content/uploads/2012/03/gsmanfcuiccrequirementsspecificationversion20.pdf