

## BasicNFC : programming NFC capabilities into the contactless BasicCard

Patrick GUEULLE

NFC (Near Field Communication) is a much promising concept that allows short range contactless communications between various kinds of smart objects (more details : [www.nfc-forum.org](http://www.nfc-forum.org)).

The most popular NFC-enabled objects are mobile phones (or smart phones), and of course NFC tags. A tag is a contactless smart card (other form factors are also available) that can be read or written by other NFC objects. Technical specifications are released by the NFC Forum, explaining how to communicate with the tags, and defining standard data contents, known as NDEF (*NFC Forum Data Exchange Format*) messages. It is highly desirable to follow them properly, in order to guarantee seamless interoperability throughout the NFC ecosystem, but please keep in mind that *"NFC Forum and the NFC Forum logo are trademarks of the Near Field Communication Forum"*.

Most tags (namely Types 1 to 3) are rather simple memory arrays that can be configured as "read-only" or "read-write", usually in an irreversible way. They are quite cheap, but their EEPROM capacity is fairly low and they have little or no security features.

Many NFC tags are made from Mifare Ultralight (Type 2) or Mifare Classic chips (NXP), but Topaz-based tags (Innovision) are also available (Type 1).

Especially well suited to demanding applications, the hardware platform of "Type 4" NFC Forum tags is a contactless ISO 7816-4 smart card with much more memory, usually from the DesFire or JCOP families (NXP).

The contactless BasicCard (ZC7.5), however, complies with the same low-level technical requirements. Being an "open operating system" smart card, it can relatively easily be programmed in such a way that it will behave much like a "Type 4" NFC tag (without being formally approved by the NFC Forum, though).

Some of the most exciting applications of such high-end NFC tags will probably make use of the "active contents" principle. In short, the memory contents of the tag can be modified, not only by another NFC object, but also by a software program which is running inside the tag itself, and therefore by proprietary (i.e. non-NFC) commands. Very powerful indeed !

Thanks to its advanced cryptographic features, the BasicCard could bring strong security mechanisms to such applications, while being able to communicate with existing NFC objects, typically smart phones.

The "card" source code which is provided with this application note (BasicNFC.bas) should be understood as a demonstration of how a few lines of ZCBasic can allow a contactless BasicCard to be read, written, and possibly write-protected, by using the very same commands than with a "Type 4" NFC tag. No claim is made whatsoever about strict compliance with all or part of any NFC Forum specifications. It will be the responsibility of the user to carry his own suitability evaluation, and to obtain any required approvals, should he wish to develop a real-world application.

This being said, the card program has been intensively tried with the "contactless and NFC SDK" from SCM Microsystems ([www.scm-micro.com](http://www.scm-micro.com)) and of course with the Omnikey 5321 dual-mode reader that comes with the contactless BasicCard kit. Some tests have also been made with several NFC enabled mobile phones and smart phones, mainly from Nokia.

Some of them, however, are only able to read NFC tags in general, and cannot write into them.

For convenience, two small "terminal" programs are provided to help writing relevant NDEF contents into (only) the BasicNFC tag : VC4.bas writes a sample vCard (with the author's contact details !), and SP4.bas writes a sample "Smart Poster" which should cause the smart phone to access the [www.acbm.com](http://www.acbm.com) web site. Here, one will find some articles describing (in the french language) other very unusual applications of the BasicCard...

Of course, do feel free to overwrite, as often as needed, one NDEF contents with another, as long as the tag is not switched to "read-only" mode by writing suitable bytes into its "Capability Container" (E103). Should this happen, please remember that as long as the BasicCard is left in TEST mode, there is a way back : just load the same BasicNFC application into the card again, or even reuse it for a completely different purpose.

Now, you are most welcome to write your own NFC applications from this starting point, or to simply add some NFC capabilities to an existing BasicCard application using its own commands set.

**Patrick GUEULLE** graduated in 1976 from EFREI (Ecole Française de Radioélectricité, Electronique et Informatique) as a dipl. engineer.

Working as a freelance consultant and technical writer (please visit [www.dunod.com](http://www.dunod.com)), he became strongly involved with smart cards in the late 1980's.

Since the very first days of the "Professional" version, he has used the BasicCard as an extremely powerful investigation tool, to assess the security and interoperability of the most popular smart card applications : health, banking, transportation, telecommunications, access control, contactless, and so on.

As a journalist, Patrick attends every year the CARTES & IDentification show in Paris, on behalf of various leading european magazines.

Contact details : p (dot) gueulle (at) wanadoo (dot) fr