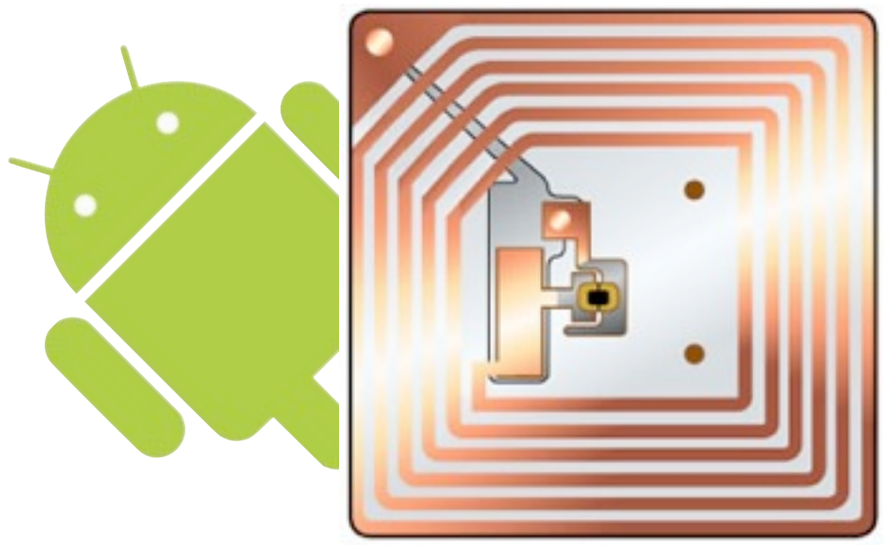
NFC & RFID with Android



Tod E. Kurt, ThingM

Where 2.0 2011, Santa Clara, CA

What is this talk?

Why you should care about RFID & NFC

Overview of what RFID & NFC is technically

How Android implements NFC

What Android can and cannot do

Some existing Android apps

Tips on how to add NFC to your Android app

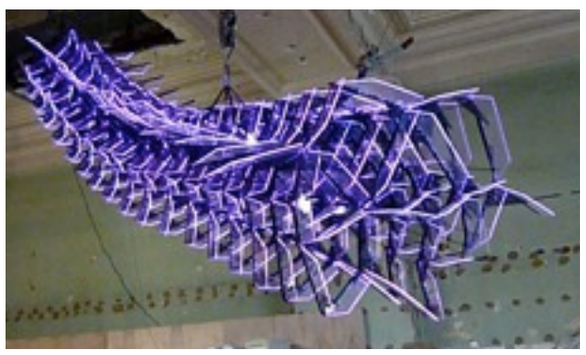
Non-Android NFC hacking

Who is this guy?

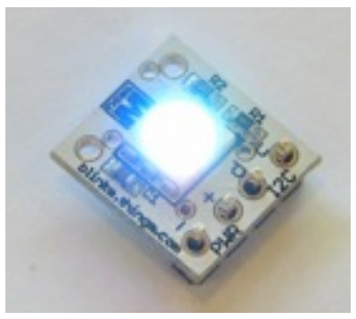
@todbot does...

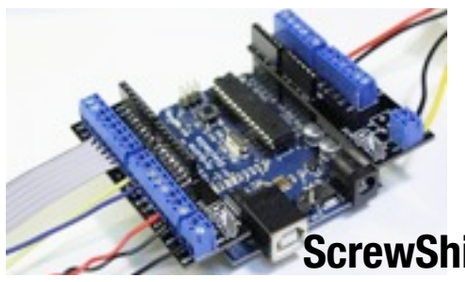
THING M

Crystal Monster



BlinkM Smart LEDs





ScrewShield

Wiichuck adapter

Spooky Arduino

CRASHSPACE.ORG

I'm Tod, aka "todbot". I'm a professional tinkerer.

I founded ThingM with Mike Kuniavsky five years ago. We're a ubiquitous computing device studio, a micro-OEM, producing a range of "Smart LED" products called BlinkM.

I've written articles for MAKE magazine, had projects featured on MAKE:TV, and wrote the book on hacking the Roomba robot vacuum.

I've been involved in the Arduino community for about five years too, and have produced a set of instructional material and hacking products.

Finally, I'm active in the local Los Angeles hacker community. In 2010 I co-founded CRASH Space, the first LA hackerspace. And I work with local Los Angeles artists to help them add technology to their works.

Why Should I Care About RFID?

Exxon SpeedPass

Mastercard PayPass

Identification

Financial Transactions

Asset tracking

Supply chain

SF Muni Clipper pass

Access control

First, how many have played with RFID tags? How many with NFC on Android?

NFC is a type of RFID.
RFID tech is being used increasingly for identification & financial transactions.
As keys to open locks of all kinds.
As the mobile phone has become a “convergence” device for other portable electronics,
so too it may become a universal “keyring” for RFID applications.

sf muni pic: http://www.flickr.com/photos/jlkinsel/5084445802/

Why Should I Care About NFC?

Some of the things NFC promises...

Some of the promises:
one-touch setup of WiFi & Bluetooth
simple touch-based data exchange
PC logins
car personalization
smart posters

http://www.nfc-forum.org/events/oulu_spotlight/Technical_Architecture.pdf
http://www.nfc-forum.org/aboutnfc/tech_enabler/
http://www.nfc-forum.org/aboutnfc/nfc_in_action/

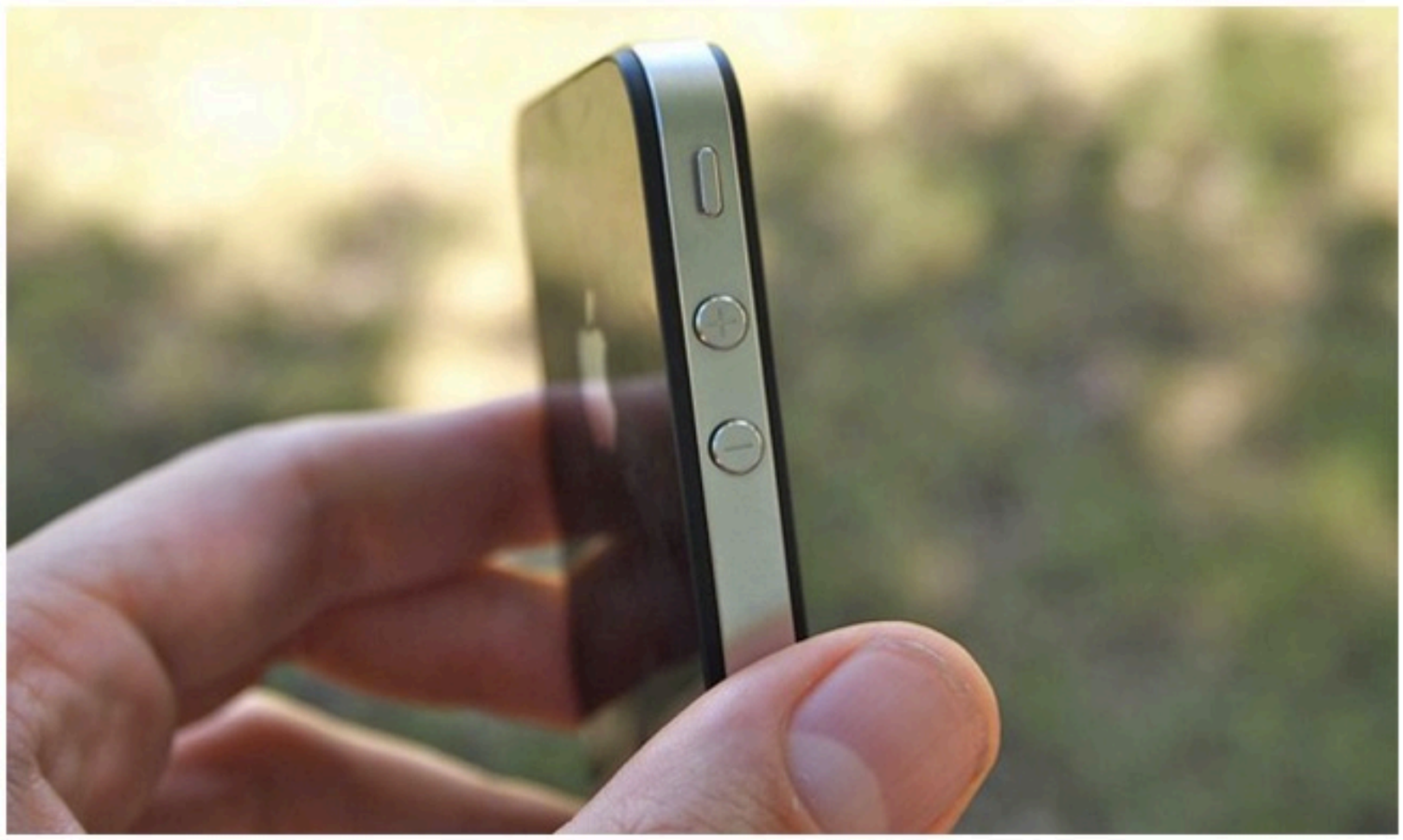
Also...

iPhone 5 NFC rumors take the stage again following new report

By: Zach Epstein | Mar 21st, 2011 at 03:20PM

View Comments

Filed Under: Mobile, Rumors

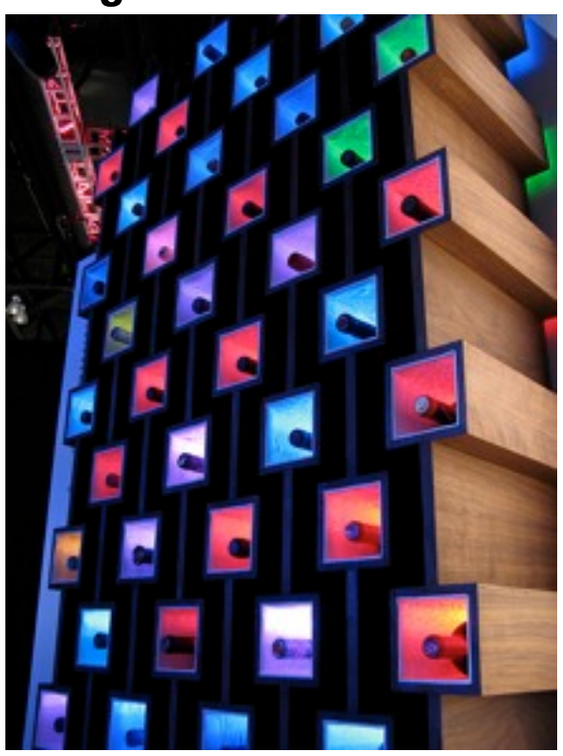


Rumors surrounding an NFC-equipped iPhone from Apple date back to last summer, when Apple hired NFC expert Benjamin Vigier as its Commerce Product Manager. Speculation surrounding how Apple might use NFC

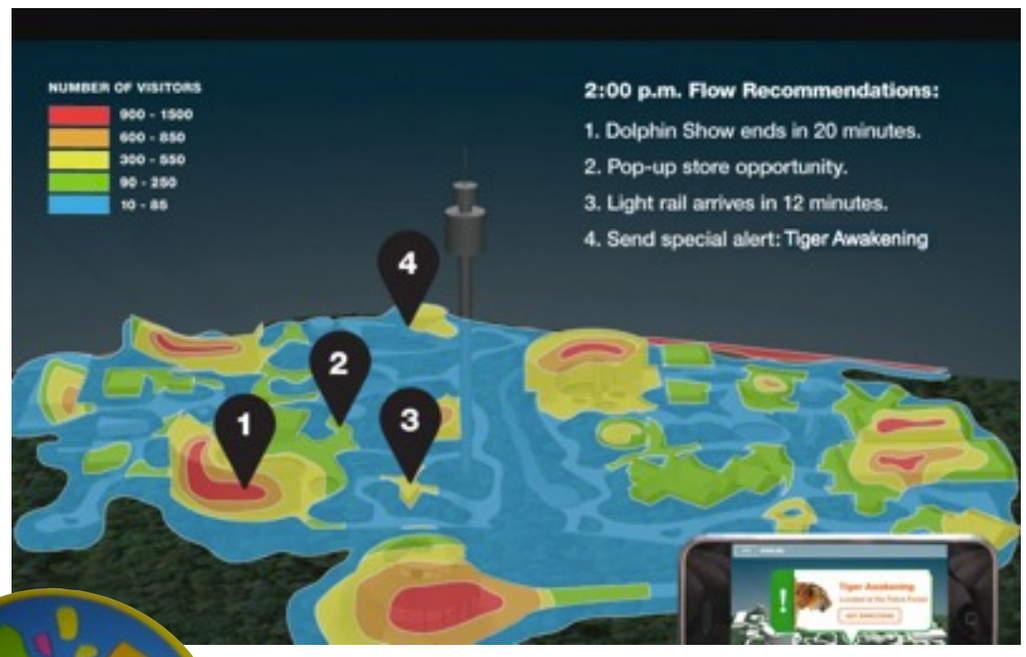
If the rumors about the next iPhone are true, we could see a flood of NFC applications in the near future.

Why I like RFID

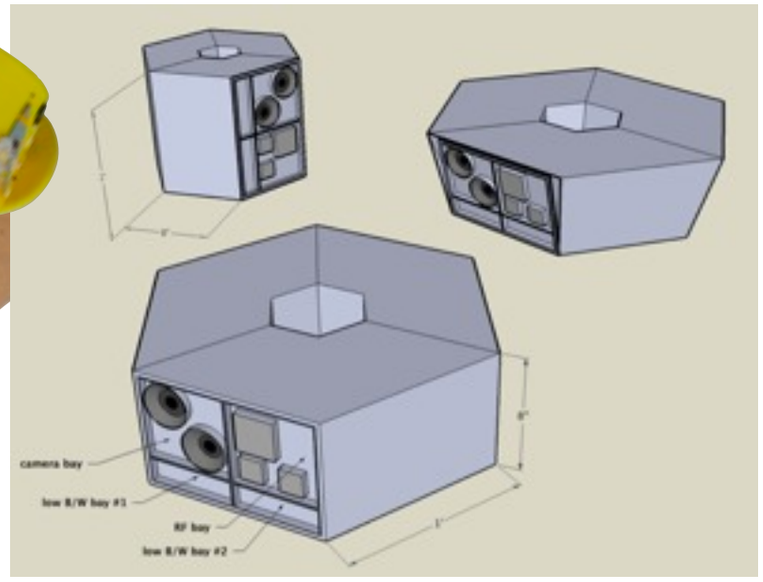
ThingM: WineM



AFK: SeaWorld in Dubai



ThingM: Ghost Tours at Henry Ford



A ThingM prototype, I designed a high-density RFID reader network for WineM, a winerack you can ask questions of. It knows what wine is in it and where it's located. Each wine slot has an RFID reader. Each wine bottle has an RFID tag.
When a wine bottle is inserted, the winerack registers that fact.
http://winem.thingm.com/

For the Henry Ford Museum, we prototyped "Ghost Tours" where visitors had "magic tickets" that created an interactive narrative flow on top of existing museum exhibits.

Another startup I co-founded was AFK, with Ben Cerveny (Bloom) and Kevin Slavin (area/code).
AFK focused on building platforms for spatial interaction.
We worked with Busch Entertainment (SeaWorld/Busch Gardens) on new projects domestically and in Dubai.
One of the things I designed was an active and semi-active RFID ticket sensor network that was to blanket an entire park.

RFID

Okay so let’s talk about what RFID actually is.

RFID is Easy

RFID tag – just a serial number, a unique ID

UID 32-bit or 56-bit

Some tags UP TO 4kB! (wow!) of writeable data

I used to think RFID tags stored lots of data.
And that the RFID tag had some meaningful communication with its reader.
No. At its basic, RFID is just a barcode.

RFID tags are just another kind of machine-readable number.
Like barcodes, or QR codes, or magstripes.

All RFID tags have a permanent UID. Some tags have an additional writable area of 64bytes to 4kB.
Some tags have a crypto engine for doing key exchanges, but those are in the minority.

Why RFID instead of...

...barcodes
– can have a lot more data, no ugly barcode

...QR codes
– can write data, no camera lag, no ugly qr code

...Bluetooth
– cheaper, low-overhead, easier setup

...WiFi / GPS localization
– cheap, definite, closely-spaced location

What RFID is Not

NOT localization

NOT proximity detection

NOT fast data transfer

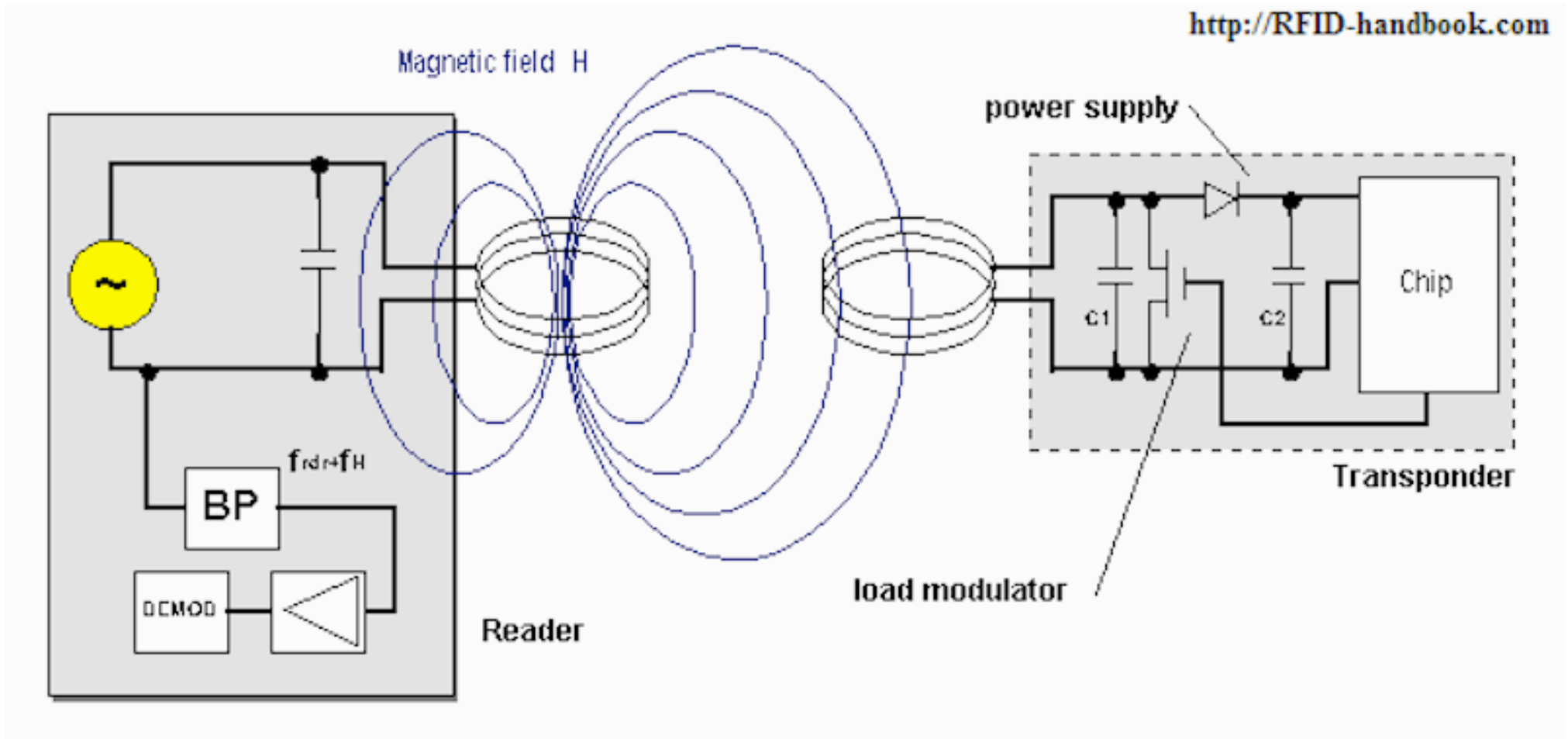
NOT secure (for non-smartcard)

Be careful using it for identification, use it instead for fun

Not localization - no position data can be inferred from a tag read
Not proximity detection - you can't tell how far away a tag is from a reader
Not crypto

It's easy to use RFID but hard to use it securely. So eschew the use of it for sensitive information, instead use it for entertainment and fun.

How RFID works



“reader”

expensive ($10)

“tag”

cheap ($0.10)

This is the only schematic in here, promise.

The reader does two things:
- generate a high-power RF field to power the tag
- officiate the protocol between the two devices

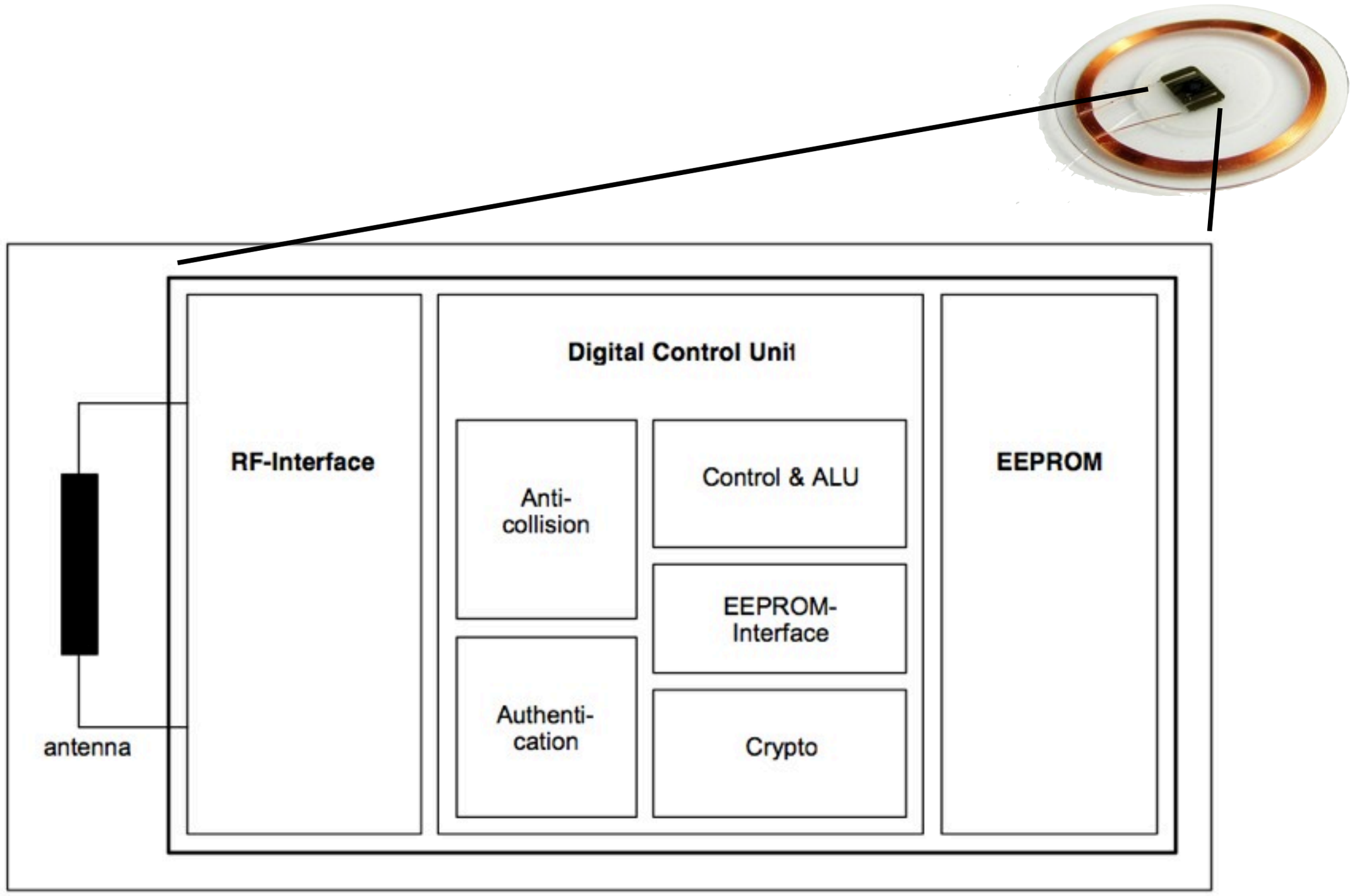
Most tags are “passive”. They have no power source. Instead, powered by the reader.
Power and communication are transmitted inductively, like a wireless charging sytems.

Readers control the data transmission. Readers energize the tags.

Data rate is between 100 kbps and 800 kbps.
RF carrier is at 13.56MHz for NFC RFID.

http://www.rfid-handbook.com/rfid/types_of_rfid.html

Passive Tag Internals



The insides of these cheap tiny tags.
It's essentially three sections: an RF interface, a memory, and a controller joining the two.

Some tags have rewritable EEPROM, some just have ROM.
Some have only a few bytes (just enough for the UID), some have up to 4kB.

http://www.rfid-handbook.com/rfid/types_of_rfid.html

Some Interesting RFID Examples

Waterpark ticket

day-pass vs season pass

age-based restrictions

payment of food, beverages, merchandise

Tickets in the form of RFID wristbands are becoming increasingly popular in amusement parks.
Because they are waterproof and wrist-attached, people can carry them anywhere.

Use their RFID bracelet to lock up their personal effects.

Since visitors carry them everywhere, they can be leveraged for other purposes.
Visitors can purchase food and merchandise. Alcohol served only to non-minors.

Casino Chips Theft Fail

man steals $1.5M in chips, cashes them in for $0 and jail

“RFID can void the stolen chips, like a registration that’s no longer valid,” Kendall said.

“When we manufacture RFID-embedded chips and send them to a casino, they’re not worth anything until they register the codes. Until then, they’re nothing but freight.”

Dec 2010, guy walks in with a motorcycle helmut on, walked up to craps table, and walked out with $1.5 million in chips. The casino unregisters the chips. Thief comes in to cash some in, security grab him.

http://www.minyanville.com/businessmarkets/articles/bellagio-anthony-carleo-rfid-las-vegas/2/3/2011/id/32595
image: http://news.cnet.com/2009-7355_3-5568411.html?tag=mncol;txt

NFC

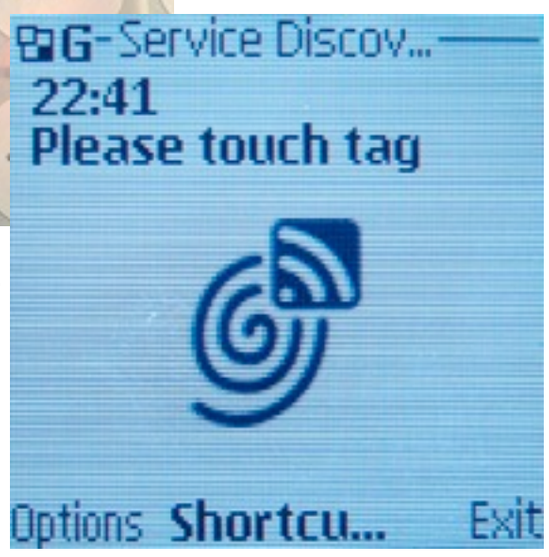
And what’s NFC then?

NFC: Near Field Communication

web-like semantics for RFID

Built on existing RFID tech

Nokia 3220 NFC



NFC products available since 2005

Multi-part, mime-typed, textual data

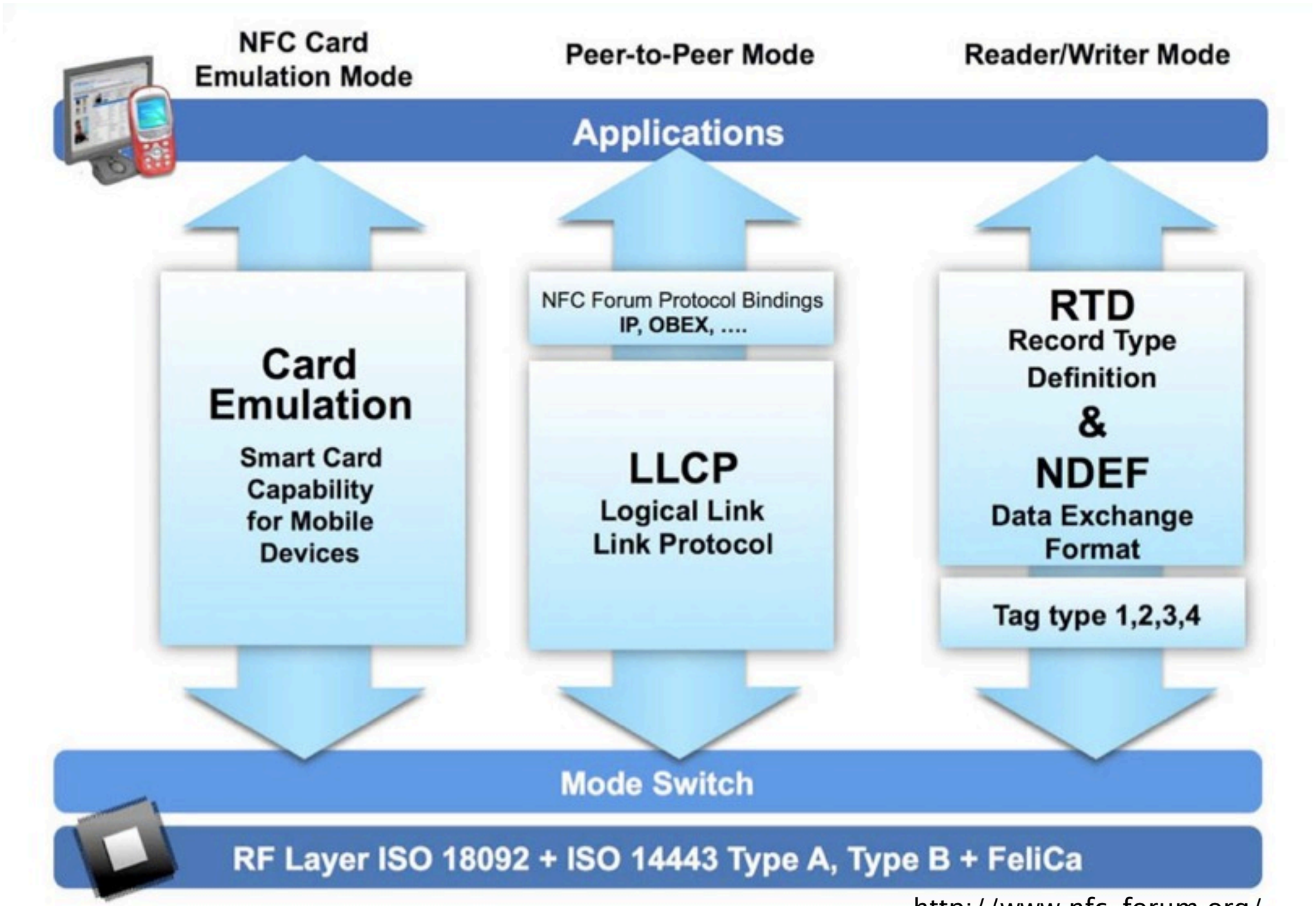
Devices can have 3 modes:

- tag reader/writer
- tag emulation
- peer-to-peer data transfer

Instead of just using the UID, a key into a database,
now can have interesting self-contained data

image: http://www.elasticspace.com/2005/12/nokia-3220-nfc

NFC Technical Architecture



http://www.nfc-forum.org/

image: http://www.nfc-forum.org/events/oulu_spotlight/Technical_Architecture.pdf

NDEF: NFC data exchange format

some example NDEF formats

Type name format	Type name	Description
MIME	text/x-vCard	Business card
MIME	text/x-vCalendar	Calendar note
NFC Forum RTD	urn:nfc:wkt:Sp	Smartposter
NFC Forum RTD	urn:nfc:wkt:U	URI record
NFC Forum Ext Type	urn:nfc:ext:nokia.com:bt	Bluetooth record (for printing/image frame)

http://wiki.forum.nokia.com/

In addition to the low-level protocol specs,
NFC also defines a set of mime-types and microformats for concisely embedding certain types of information, like URLs, where it has codes for common strings like “https://www.”

image: http://wiki.forum.nokia.com/

Some cool NFC ideas

Tap Your Top10 – Send top 10 list to DJ by tapping phone

HouseMood – Tap your house so it knows your mood

HiRes 4SQ – Precise, hyper-dense checkins with foursquare

free business models here, no charge.

NFC Capabilities on Android

Currently available Android NFC phones: Google Nexus S

Use Android 2.3.3 (API Level 10) as the NFC APIs drastically changed from 2.3.2.

New Intent Filter and TechFilter APIs for registering interest in types of cards, types of NDEF messages, types of NFC events

What works now on Android?

Tag reader/writer

Tag emulation (of certain NFC NDEF tags)

P2P communication (Android-specific)

What doesn’t work

Tag emulation of Smart Cards

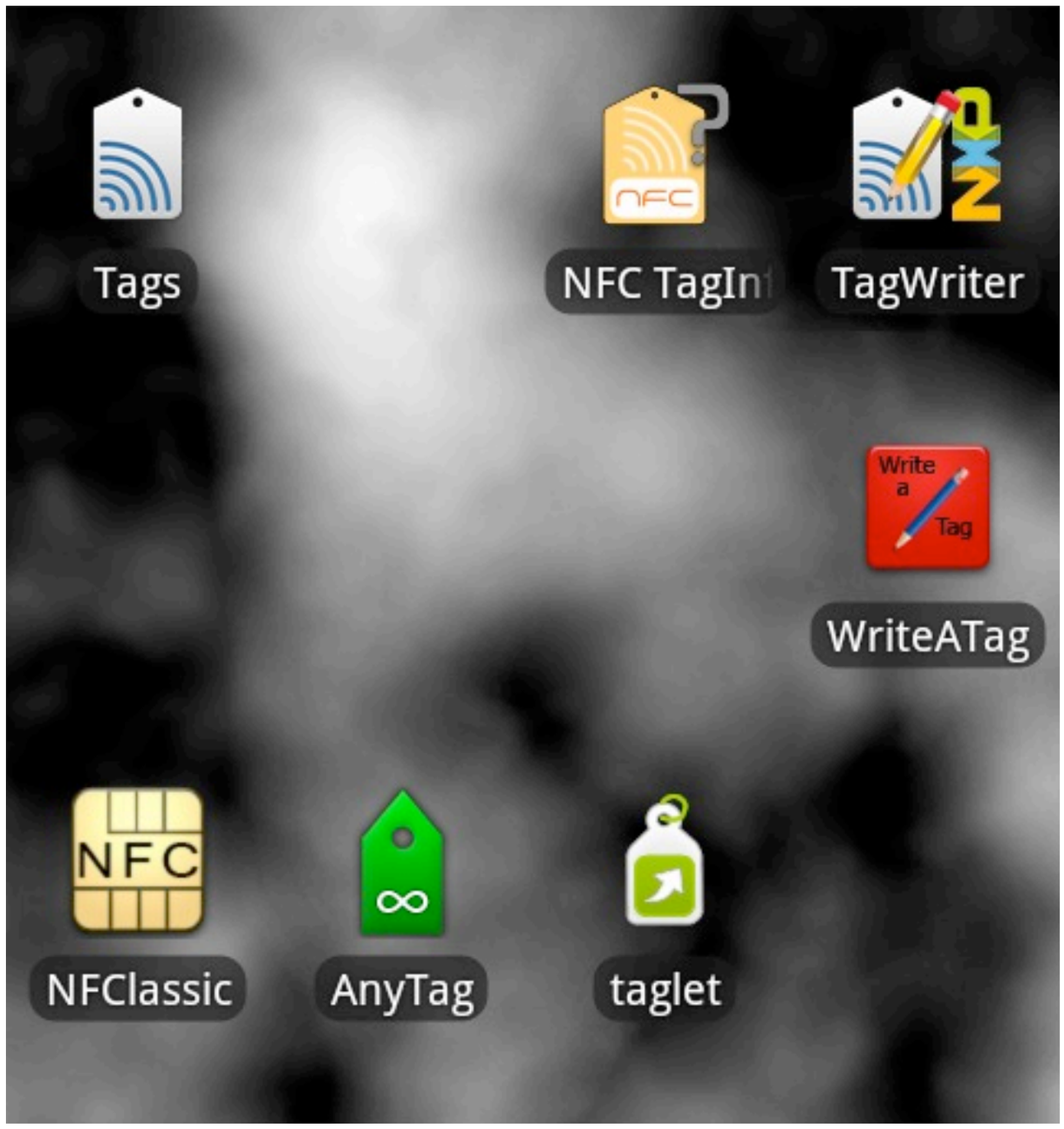
Peer-to-peer with Nokia NFC phones

Nexus S NFC Hardware

Thursday, April 21, 2011

Nexus S NFC antenna in back cover; two spring-loaded contacts make the connection.
The Secure Element chip is on the blue board for tag emulation.
It’s a SmartMX combined into the same package as the PN544 NFC controller

Current App Landscape



I’ve been looking at them mostly for testing of NFC & RFID

taglet & AnyTag

“bit.ly for RFID tags”

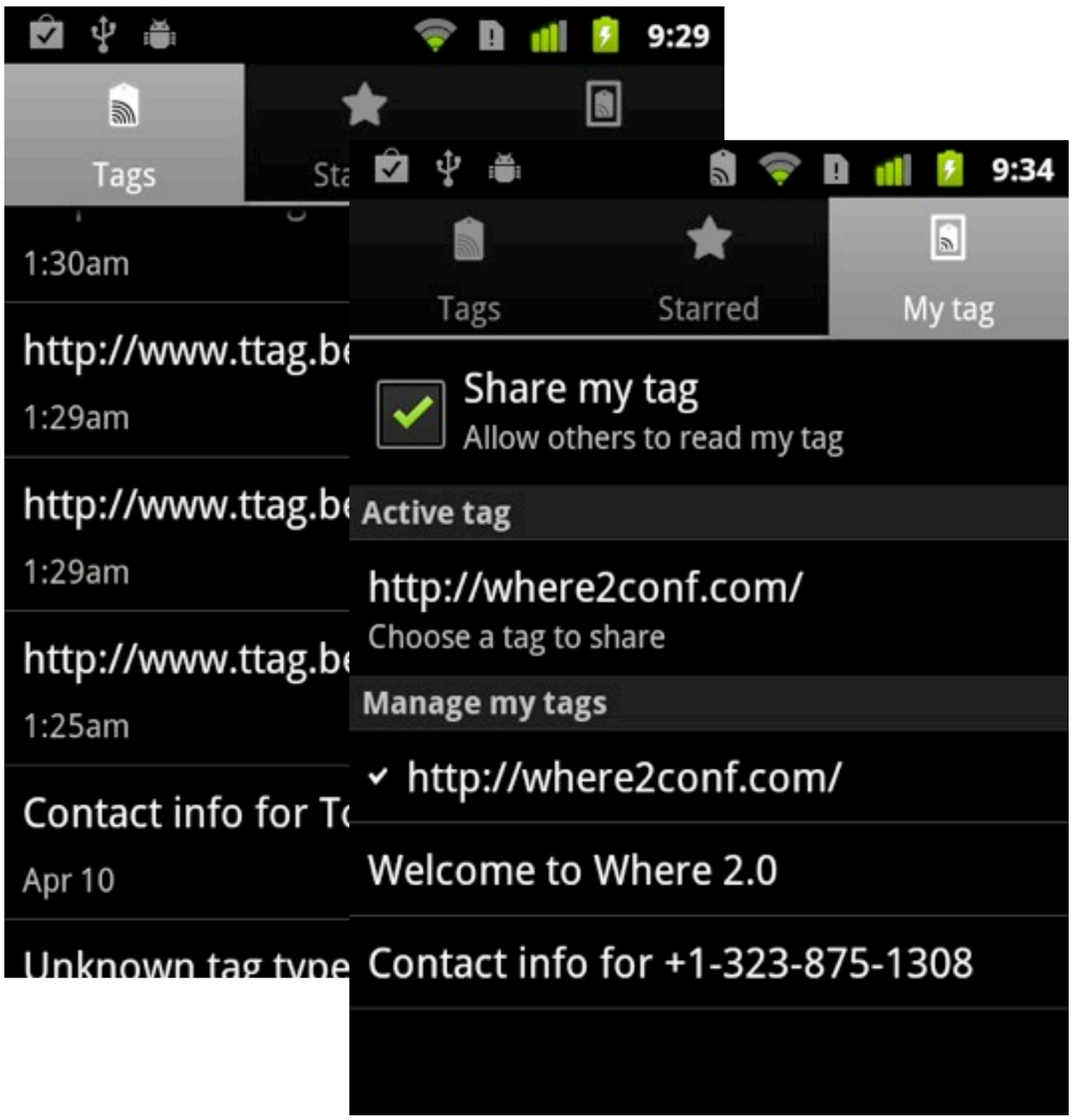
maps UID –> URL

works with any tag phone can read

but both don’t seem to work on 2.3.3

AnyTag is open source : http://code.google.com/p/anytag-android/
taglet is implemented as a web app somehow.

Tags App



System App

Two functions:

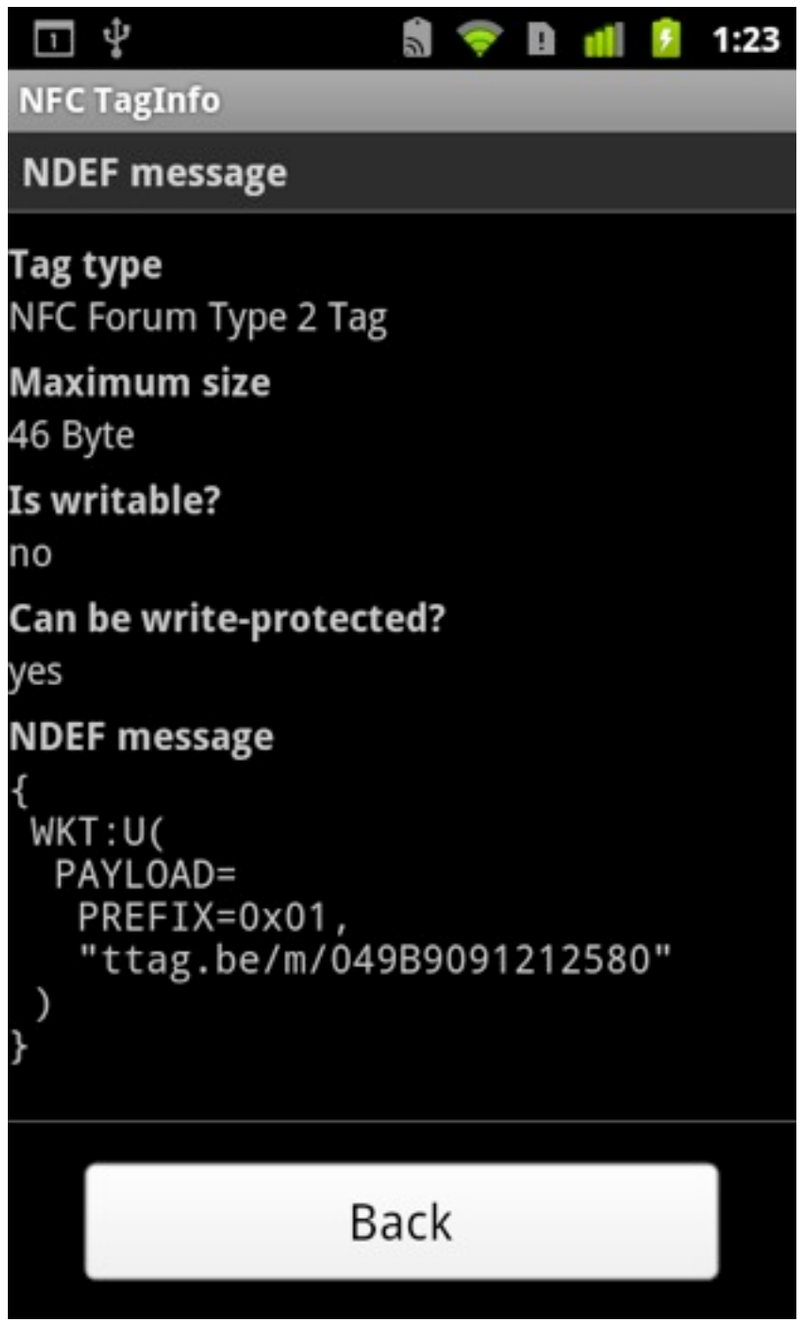
- tag reader

- tag emulator

Makes sharing contact info & URLs easy

NFC TagInfo

most useful



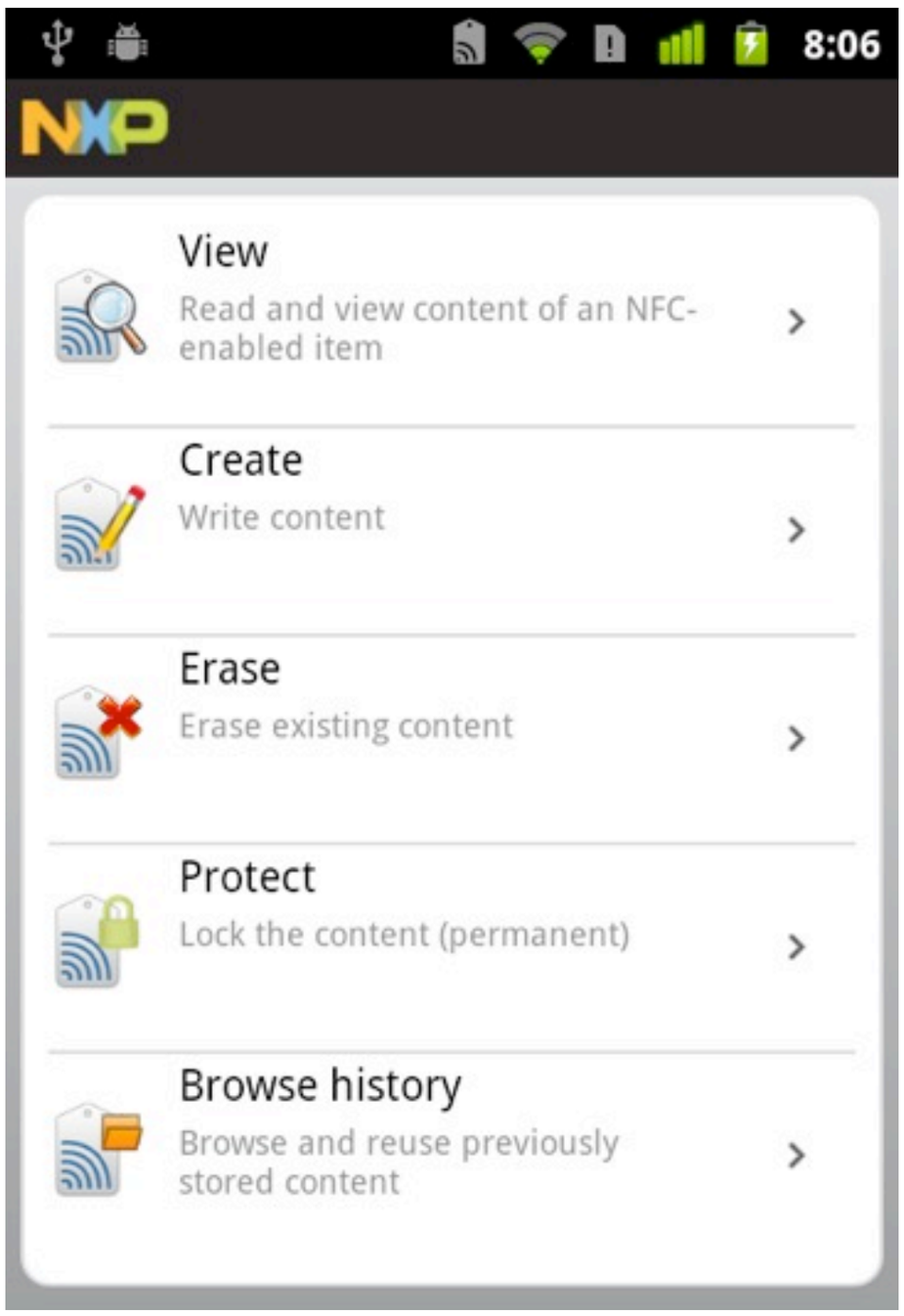
They recompiled the SDK to get access to previously hidden APIs.

These guys are good.

http://www.nfc-research.at/

NXP TagWriter

lets you format tags for NDEF use



NXP produces many RFID chips and reader products.
TagWriter can “back up” NFC tags.

Here is an example of TagWriter reading one of the 46-byte read-only Touchatag tags.

NXP TagWriter

And here's an example of TagWriter writing to a 1kB Mifare tag.

App Demos

Let's try to show some demos...

Show some of these apps in action on the video camera.

Developing NFC on Android

Disclaimer: I'm not a big Android programmer.

Good docs at http://developer.android.com/guide/topics/nfc/ go read them.

Instead, look at the process from a high level

And at the lower-level setup and gotchas

Okay let's look at what it would take to add RFID/NFC capability to an app.

Quick Android SDK Setup Intro

Android apps are written in Java using Eclipse IDE

Install Eclipse (or other favorite IDE)

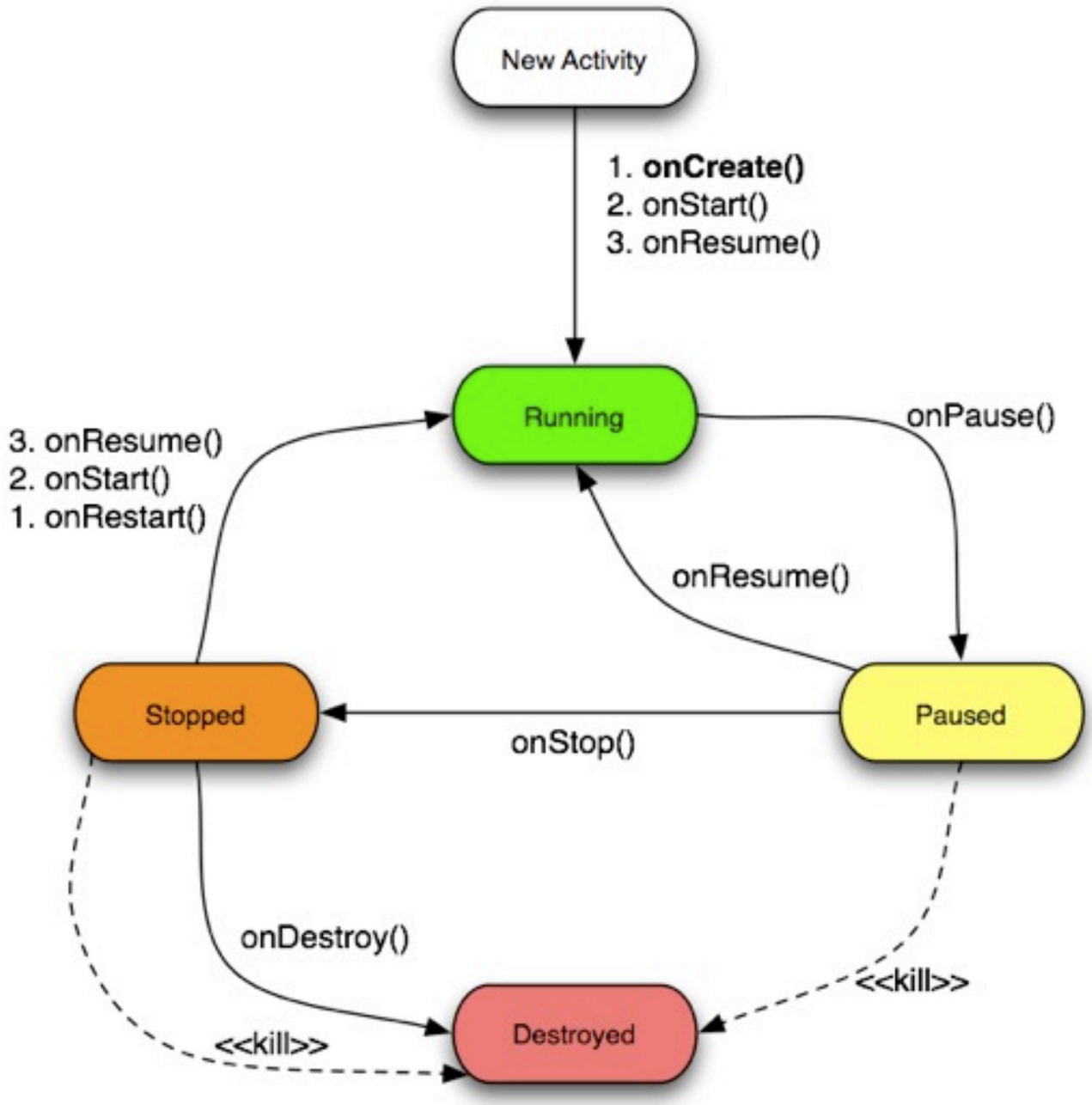
Download Android SDK

Hook Android SDK up to Eclipse

Tell SDK to download needed extra packages

Then you can start a new Eclipse Android project

App Activity lifecycle



Apps have at least one Activity

Activities triggered from system events, “intents”

Activities are paused & resumed by Android system

If you’ve never programmed in Android before, here’s the basic lifecycle of the primary chunk of code you write: the Activity

image: http://stuffthathappens.com/blog/2008/11/01/android-activity-lifecycle/

Main Steps to add NFC

- Edit app's `AndroidManifest.xml`, set:
  - Minimum SDK version
  - Hardware permissions
  - Intent filters
- Two ways to work:
  - Intent Dispatch – run your Activity on tag presence
  - Foreground Dispatch – intercept tag intents

Every Android app has an AndroidManifest.xml file that describes needed resources and permissions. An app's activities, intents and services and permissions are declared in the manifest file

http://stackoverflow.com/questions/4815718/getting-the-nfc-hardware-id-in-android

Permissions in Manifest

Set SDK version to get to NFC APIs:

```
<uses-sdk android:minSdkVersion="10"/>
```

Request permission from the user to use NFC hardware:

```
<uses-permission android:name="android.permission.NFC">
```


These are the two most important things to add to your code.
In your app's AndroidManifest.xml

Intent Filter in Manifest

NFC intent filters tell Android your Activity can handle NFC
And let you control what kind of tags your Activity sees

```
<intent-filter>
  <action android:name="android.nfc.action.NDEF_DISCOVERED"/>
  <data android:mimeType="mime/type" />
</intent-filter>


<intent-filter>
  <action android:name="android.nfc.action.TECH_DISCOVERED"/>
  <meta-data android:name="android.nfc.action.TECH_DISCOVERED"
             android:resource="@xml/nfc_tech_filter.xml" />
</intent-filter>

<intent-filter>
  <action android:name="android.nfc.action.TAG_DISCOVERED"/>
</intent-filter>
```


There are three different intents you can register for:
- NDEF_DISCOVERED – What kind of NFC-formatted NDEF packet you're looking for
- TECH_DISCOVERED – What kind of RFID tag you're expecting
- TAG_DISCOVERED – Is a tag present or not

Intent Filter

Can even filter on NFC mime-type

```
<intent-filter>

  <action android:name="android.nfc.action.NDEF_DISCOVERED"/>
  <data android:mimeType="text/x-vcard"/>

  <category android:name="android.intent.category.DEFAULT"/>

</intent-filter>
```

Seems you need to have “category” or it doesn’t work.

TechFilter

Filter for what kind of tag hardware you care about

```
<resources
xmlns:xliff="urn:oasis:names:tc:xliff:document:1.2">
    <tech-list>
        <tech>android.nfc.tech.IsoDep</tech>
        <tech>android.nfc.tech.NfcA</tech>
        <tech>android.nfc.tech.NfcB</tech>
        <tech>android.nfc.tech.NfcF</tech>
        <tech>android.nfc.tech.NfcV</tech>
        <tech>android.nfc.tech.Ndef</tech>
        <tech>android.nfc.tech.NdefFormatable</tech>
        <tech>android.nfc.tech.MifareClassic</tech>
        <tech>android.nfc.tech.MifareUltralight</tech>
    </tech-list>
</resources>
```


Filter for what kind of tag hardware you want to look at.

Get Tag Data

In `onCreate()` if using intent filters,

or anywhere using foreground dispatch

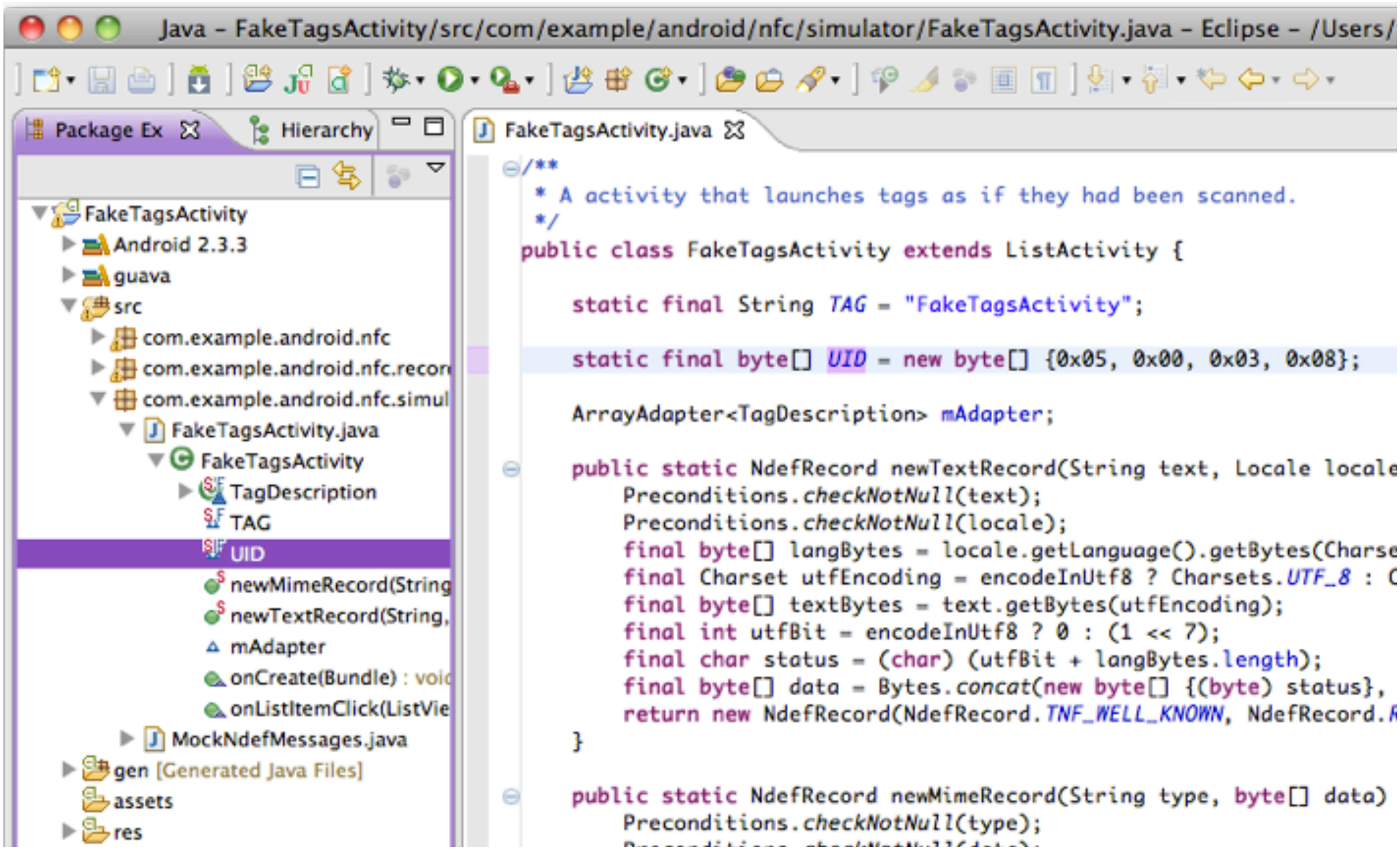
```
Intent intent = getIntent();

NdefMessage[] msgs =
  intent.getParcelableArrayExtra(NfcAdapter.EXTRA_NDEF_MESSAGESs);

for (int i = 0; i < msgs.length; i++) {
    NdefRecord[] records = msgs[i].getRecords();
}
```

With all that setup, just getIntent() then get an array of NdefMessages containing an array of NdefRecords.

FakeTagsActivity



Like most interesting sensors on smartphones, you can't use the simulator to test. You test on the device. Google provides a trick around this.

Hacking NFC

not on Android

Get a USB or serial reader

Get some tags (SF Muni Clipper, your prox card, etc.)

Get some apps

Hook it up to your PC or Arduino

If you want to explore RFID & NFC outside of Android (which is useful for debugging Android), you should get some reader hardware.

Touchatag

http://touchatag.com

Inexpensive ($40) USB NFC reader

Comes with 10 read-only 64-byte tags

Works with libnfc

The tags it comes with are read-only, but pre-formated with NFC URL data.

Proxmark

http://www.proxmark.org/

GPL RFID hardware reader

Build it yourself, if you're hardcore

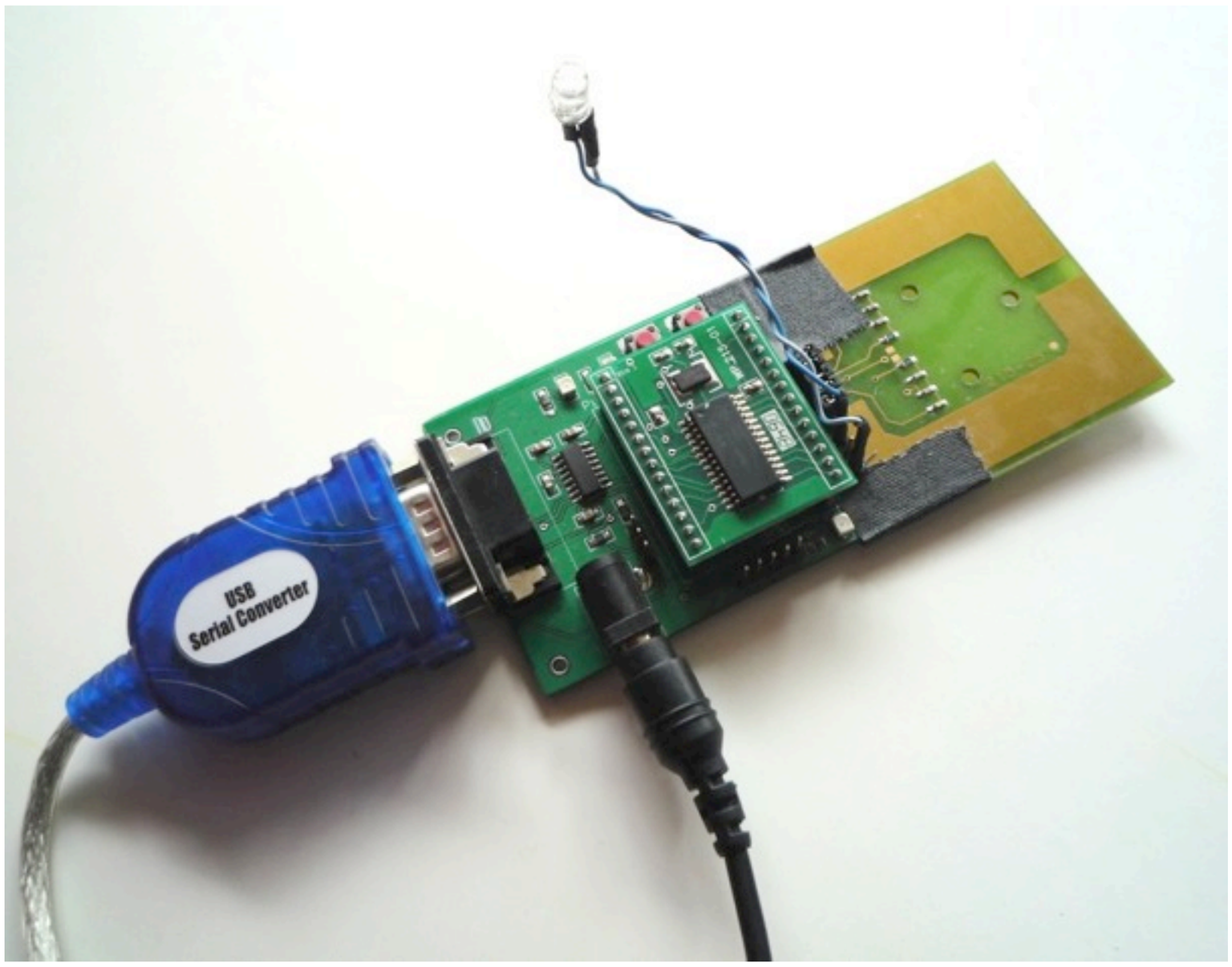
Read/emulate any RFID tag

$300

Open source and awesome, is used to explore possible exploits to RFID and NFC.

SonMicro RFID

http://sonmicro.com



13.56 MHz RFID reader

Libraries for Processing & Arduino

Read/write tags

Limited NFC, no emulation

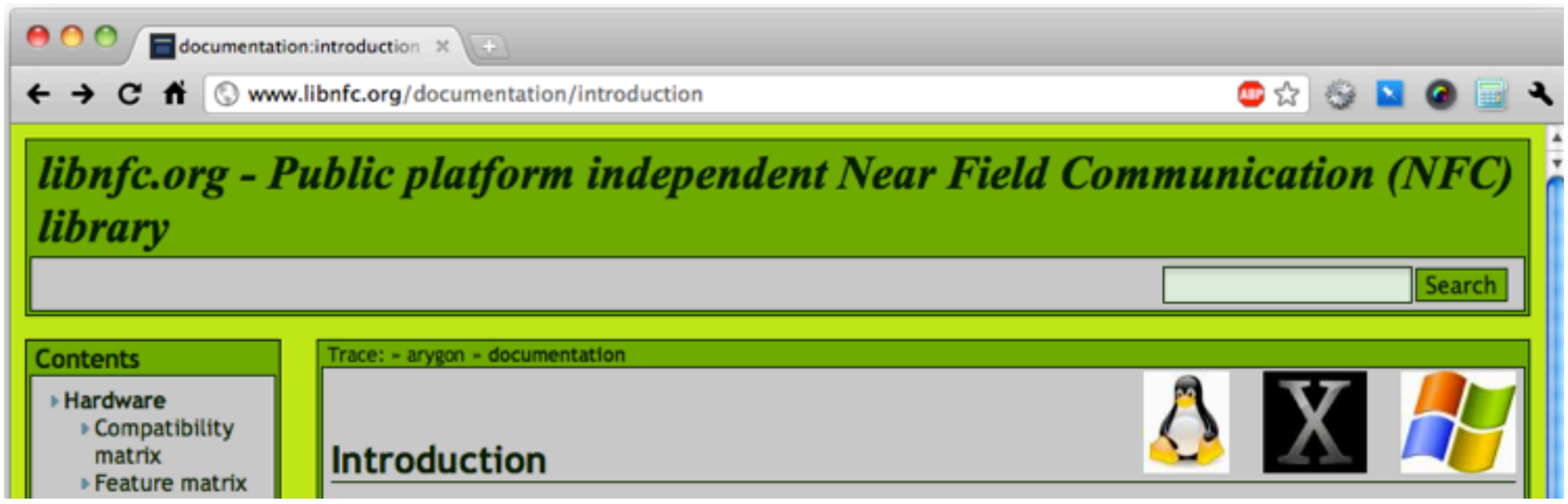
$30

avail from SparkFun

At SparkFun at http://www.sparkfun.com/products/10126
should probably also get: http://www.sparkfun.com/products/10162

LibNFC

http://www.libnfc.org/



Multi-platform library for NFC exploration

Works with most all NFC/RFID USB readers

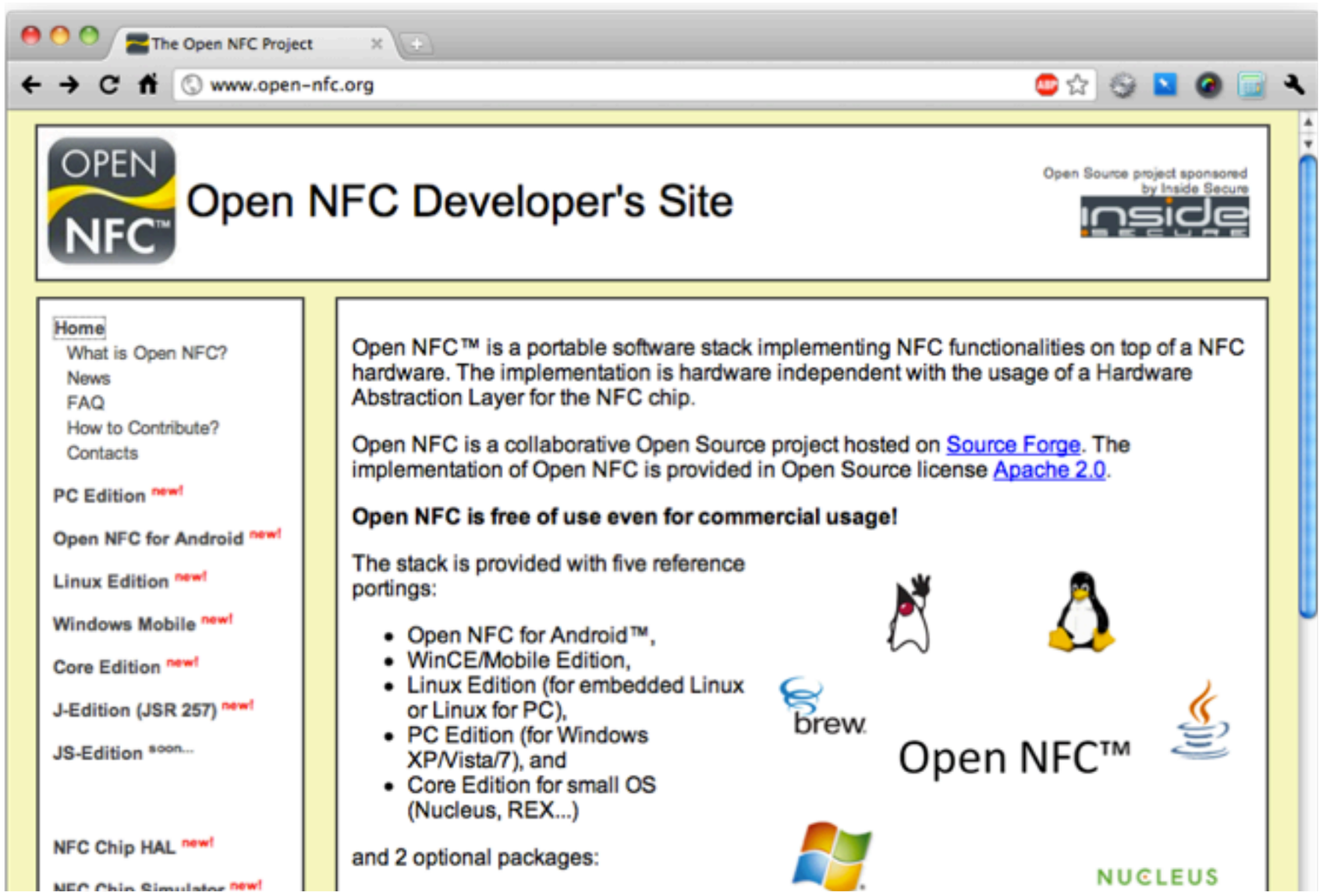
Understands most all NFC/RFID tag types

Active developer community

http://www.libnfc.org/

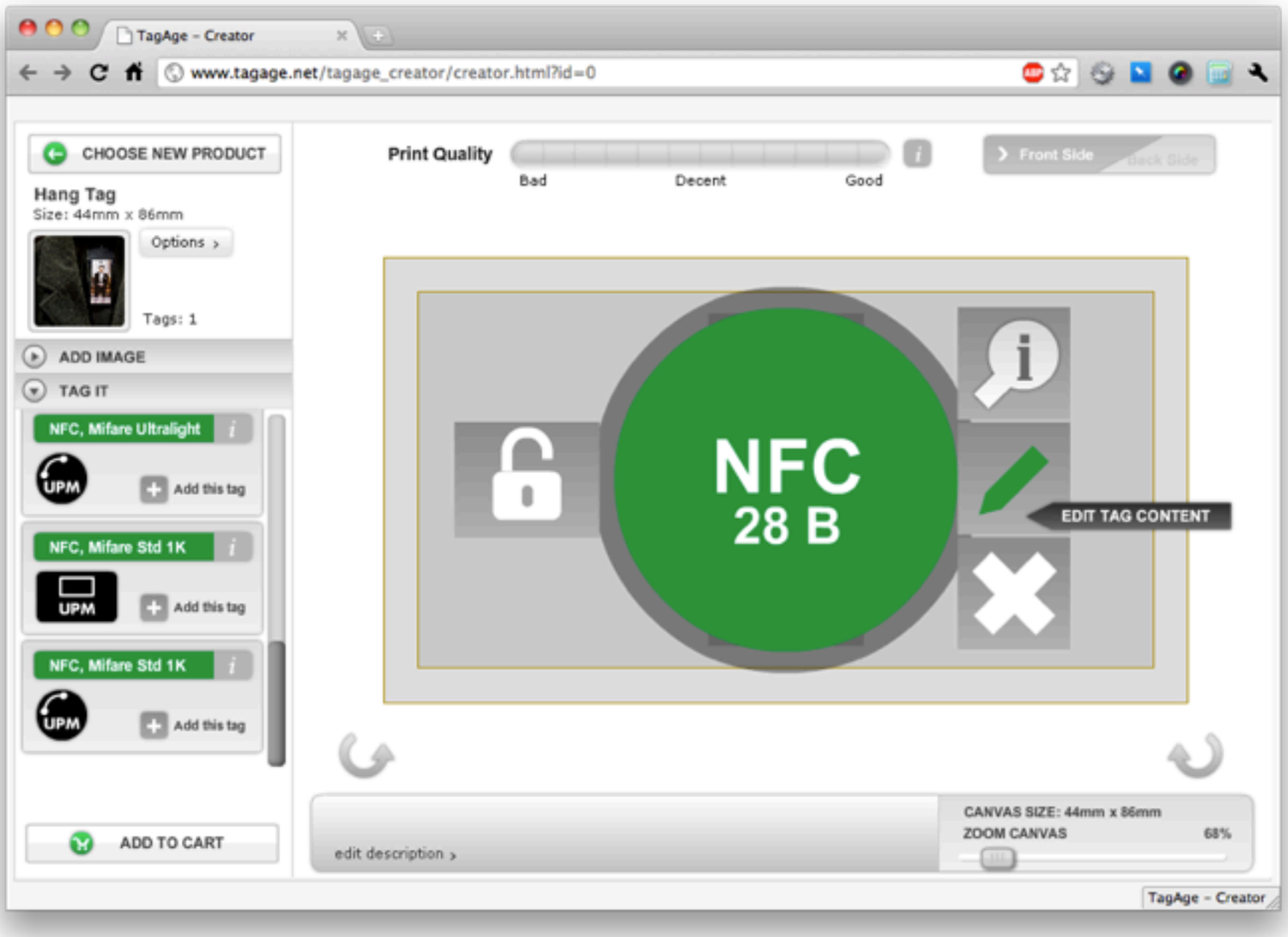
Open NFC

http://www.open-nfc.org/



http://www.open-nfc.org/

TagAge.net



Create custom NFC tags with custom graphics, all online

Print your own NFC tags, with multiple tag types.
Same web interface as online sticker makers, but also contains RFID tags.

Links

http://developer.android.com/sdk/android-2.3.3.html

http://developer.android.com/guide/topics/nfc/index.html

http://developer.android.com/reference/android/nfc/NfcAdapter.html

http://www.rfid-handbook.com/rfid/

http://www.nfc-research.at/

http://www.nfc-forum.org/

http://www.proxmark.org/

Thank You

imagine these guys with NFC tags

hat-tip to Carlyn for this video
http://www.youtube.com/watch?v=IQ6xGMSOu1E

Thank You

imagine these guys with NFC tags

hat-tip to Carlyn for this video
http://www.youtube.com/watch?v=IQ6xGMSOu1E

Tod E. Kurt
http://thingm.com/
http://todbot.com/blog/