X-Series Implantable Transponder FAQ

Transponder Information

Transponder Safety

Installation Procedure

Using X-Series Transponders

Q: What's the difference between RFID and NFC?
A: RFID is an acronym meaning Radio Frequency IDentification, and is a generic name for a range of technologies that allow things to be identified in some way using radio waves (RF). This means just about anything that communicates wirelessly can be considered "RFID", including your cell phone which has several radio transceivers which all have unique identifiers (MAC addresses, IEMI, etc.). Typically though, when someone talks about "RFID", they are generally referring to passive (unpowered) transponders (also called "tags"). Passive tags contain no battery or power source. They operate by pulling power from a magnetic field generated by a reader device, which limits their effective range. The world of passive RFID tags is a large, with a huge range of operating frequencies, data protocols, memory capacities, and features.

NFC is an acronym meaning Near Field Communication. A consortium of Nokia, Sony, and Philips originally created the NFC Forum, and the forum decides on NFC standards. Those standards are made up of two basic parts, a specific small set of passive RFID tag types (called "NFC tags") and active device communication (peer to peer). The NFC standard defines 4 different types of passive RFID tags which can be used as NFC tags, based on their memory structure and communication protocols (frequency, data encoding, etc.). So, all 4 types of "NFC tags" are just certain types of RFID tags that have been chosen by the NFC forum as "NFC compliant".

For example, a Mifare Ultralight tag is a passive RFID tag that operates at 13.56MHz and communicates using ISO14443A. The Mifare Ultralight has a memory structure that can be formatted and used as an NFC Type 2 tag. However, the Mifare S50 1K tag is also a passive RFID tag that also operates at 13.56MHz and is also ISO14443A, but it is not NFC compliant. The memory structure used by the Mifare "classic" S50 1k tag is not compliant with the NFC standard, so it is not considered an "NFC tag", even though it is sold as an "NFC tag" by many vendors trying to capitalize on all the NFC buzz. Don't believe the hype.

Q: What's the difference between x-series transponder types?

A: We sell 4 different types of x-series transponders (RFID tags); the xEM, xNT, xM1, and xIC. The xEM and xNT are sold in kit form and are preloaded into injector assemblies, and thus are sold under the xEMi and xNTi SKUs.

xEM 125khz EM4102
The xEM is a low frequency 125khz transponder based on the ATA5577 chip which has some user programmable memory and some basic security features, and allows you to program or clone EM or HID tag IDs to it with our xEM Cloner. Each xEM tag is programmed at the factory with a unique ID and set up to emulate an EM41xx style chip, which is a very common low frequency chip type. In this mode, it works with common EM41xx based readers available through many hobby electronics shops and electronics outlets. The xEM can also emulate HID ProxMark II card IDs, which are commonly used in corporate access control applications. Several commercial or "off the shelf" systems are compatible with the xEM tag, however we offer it as a "starter" transponder for people new to RFID in general. The xEM is low cost, simple to use, and we also sell an xEM Access Control unit that works beautifully with the xEM tag that enables hobbyists to cheaply and easily build simple access control type projects.

xNT 13.56mhz NTAG216
The xNT is a high frequency 13.56MHz transponder based on the NTAG216 chip. The NTAG216 has 888 bytes of user programmable memory, 32 bit password protection security features, and is both ISO14443A and NFC Type 2 compliant. You can use the xNT with both commercial systems that work with ISO14443A as well as NFC devices like mobile phones and new ISO14443A and NFC hobby electronics as well. There are several hobby electronics readers and reader kits available, including one we sell, that work with Arduino and other micro-controllers commonly

used by hobbyists and product engineers alike.

xM1 13.56mhz S50 (Mifare Classic 1K)
The xM1 is a high frequency 13.56MHz transponder based on the Mifare Classic S50 1K chip. This chip type is ISO14443A compliant but is not NFC compliant. The xM1 has 768 bytes of user programmable memory and also supports Crypto1 security features. The xM1 is supported only on some NFC devices which contain a reader chip from NXP. While the xM1 will work with any ISO14443A reader, including our PN532 reader, it cannot be expected to work reliably with all NFC devices. We supply the xM1 for people who have a specific need for this particular chip type.

xIC 13.56mhz ICode SLI
The xIC is a high frequency 13.56MHz transponder based on the ICODE SLI chip. This chip type is ISO15693 compliant but is not NFC compliant. The xIC has 128 bytes of user programmable memory but has no security features. The xIC is supported only on some NFC devices which contain a reader chip from NXP. While the xIC will work with any ISO15693 proximity reader, it cannot be expected to work reliably with all NFC devices. We supply the xIC for people who have a specific need for this particular chip type.

Q: What can I do with my transponder?

A: That depends on what kind of transpodner you have, but in general, the most typical types of applications are all variations on access control. All RFID technology centers around the ID portion… identifying something. For objects like boxes and inventory, that means counting them, keeping track of them around the warehouse and through the shipping process. For animals like pets, it means properly identifying the animal and their owner(s). For humans, it typically means replacing keys and passwords… identity as applied to access control. Dangerous Things team members use their transponders to enter their homes, unlock and start their vehicles, log into computers, etc. The specifics of how you can accomplish those actions depends on the thing you want to access, ability to hack/update it, and the transponder you have, which are all beyond the scope of this FAQ page.

The advent of NFC standards placed over certain types of RFID transponders introduces other possibilities and activities beyond access control. Transponders with user programmable memory space and other features such as security key memory protection, enable interesting applications like vCard storage (passing contact details), acting as a mobile geocache site, enabling personal digital art, storing bitcoin wallet addresses, and generally storing arbitrary binary data that is important enough to the user to keep it inside their body at all times.

Q: I shoot guns / rock climb / do martial arts / fight super villains, etc. How durable are these transponders?

A: All of our x-series transponders are encapsulated in biosafe glass, so they are not indestructible. However, the thousands of x-series tags sold that have been installed in the correct orientation and in the suggested location in the hand (between thumb and index finger), we have had no reports of any of them breaking. Outside the body, they can be shattered somewhat easily if they encounter a hard surface, particularly the edge of a hard surface. However, once installed in the body, the skin and tissue surrounding the tag do an excellent job of buffering any blunt force impacts the tag may encounter. I personally have smashed my left hand several times, and once even hit it with the head of a steel hammer, directly over my tag. So far I've had no issues what so ever.

We've also done various tests on these glass tags, including crush testing, liquid nitrogen dunk testing, and vacuum and pressure testing. In all cases, our x-series transponders successfully survived. Here is a write-up with photos and video of the various tests we've performed on our x-series tags; https://forum.dangerousthings.com/t/tests-weve-performed-on-our-x-series-tags

In December 2013 we thought we had our first customer report of a tag breaking, but after a short call and a visit with one of our Dangerous Things partners for removal, the tag removed tag appeared to be intact. It was shipped back to us where we could look at the tag under a low power microscope and determined it was not broken. The story and photos can be seen by anyone on our Facebook page (even if you don't have a Facebook account).

Q: Are x-series transponders compatible with MRI machines?

A: Yes. We have had past customers with both xEM (125KHz) and xM1 (13.56MHz) tags go through MRI machines of the 1T, 1.5T, and 3T strengths just fine. There is blurring of the image around the area of the tag, but the tag itself does not heat up or explode or get "ripped out". Also, the MythBusters were kind enough to prove this for us in season 5, episode 19 (MythBusters Revolution) by installing a 134KHz VeriChip transponder into both a piece of a pig and Kari Byron, and running them both through an MRI scan. You can clearly see the image distortion in the episode if you're interested in seeing what it does to the MRI image.

Here is a PubMed article on RFID transponder compatibility with MRI machines up to 3T; http://www.ncbi.nlm.nih.gov/pubmed/23763334 – Functionality of veterinary identification microchips following low-field (0.5 tesla) and high-field (3 tesla) magnetic resonance imaging.

There is also an MRI Safety website entry for the commercial VeriChip, sold between 2004 and 2010, to which our transponders are extremely similar.

Finally, we have our own MRI safety documentation for our x-series transponders that can be supplied to your healthcare provider if you are having issues getting an MRI done because of concerns about your x-series implant.

Q: Are there any problems using induction ovens with x-series transponders installed?

A: No. Induction ovens operate at less than 100KHz. I have tested both our xEM 125KHz tag and our xM1 13.56MHz tag with several induction ovens, both with and without cooking pots on them, and there has been no adverse effects, no heating, no destruction of the tag, etc. I tested by affixing the tag to a wooden dowel with cellophane tape, turning on the oven cooktop element to "full", then doing the following;

* placed the tag physically on the induction element for 30 seconds
* held the tag above the induction element at 1cm and 5cm height for 30 seconds each
* placed a cooking pot with water in it on the induction element and placed the tag physically on the induction element and 2cm away from the cooking pot (so the heat from the pot would not affect the test) for 15 seconds
* placed the tag at the bottom of the cooking pot (under water) for 5 seconds shortly after turning up the element to "full"

In all instances, the tag came out just fine.

Q: Will I have problems at security checkpoints, metal detectors, airport scanners, court houses, etc.

A: No. Dangerous Things founder Amal Graafstra has had transponders in both of his hands since 2005, and he's gone through hundreds of metal detectors, had metal detector wands run over his hands, and even gone through several full body scanners used at airports, and he's never had a problem. This experience has been echoed by Dangerous Things customers for years... it's just not a problem. The amount of metal in the tag is about the same as a tooth filling, so it is not enough to set off these types of security devices.

Q: How are x-series tags installed?

A: Our x-series tags are typically sold pre-loaded inside a sterile injection assembly, which is used to inject the transponder into the subdermal fascia between dermis and muscle tissue. We typically suggest they be installed into the webbing between the metacarpal bones of the index finger and thumb, resting parallel to the index metacarpal. Achieving this safely requires a steady hand and experience performing aseptic procedures. Dangerous Things prefers our customers locate one of our [professional body piercing or body modification partners] (https://dangerousthings.com/partners) to complete the installation of this product. If no partners are available in your area, you should be able to follow [this guide] (https://forum.dangerousthings.com/t/how-to-approach-a-professional) to finding a professional in your area who is willing to assist you.

Q: Does the installation procedure hurt?

A: The installation process (in the suggested location and orientation) is about as painful as giving blood, getting a bee sting, or about as painful as most typical body piercings. There is a slight sharp pinching sensation as the needle initally pierces the skin, but after that it's very easy going. We've had people actually say "that's it?" afterward.

If you'd like to see first hand (pun!) how our x-series transponders are installed and how people react, you can watch Dangerous Things founder Amal Graafstra perform several upgrades on volunteers for a Tele2 livestream event below.

Q: What about aftercare and the healing process?
A: Our x-series transponders are typically installed into the webbing between the metacarpal bones of the index finger and thumb, resting parallel to and centered on the index metacarpal, half way between the index knuckle joint and trapezoid bone. Achieving this safely requires a steady hand and experience performing aseptic procedures. Dangerous Things prefers our customers refer to our partner map to locate one of our professional body piercing or body modification partners to complete the installation of our products. If no partners are available in your area, follow this guide to find a professional in your area who may be willing to assist you.

Once an x-series tag is placed under the skin, you can expect some bruising and slight swelling. The skin wound should scab over and stop bleeding within 5 to 30 minutes. The swelling should go down within 2 to 24 hours, but bruising may remain for a few days. After swelling goes down, you should notice slightly better read range performance. After the first day, you should be in pretty good shape, happily using your tag. You can wash your hands normally and take showers, etc.

Over the two to four weeks post installation, the body will begin to encapsulate the tag with fibrous collagen tissue. To help this process along, you can take pre-natal vitamins, which help build collagen and connective tissues. During this time, it is important that you not perform any strenuous activity, put pressure on the tag, play with or poke at the tag, work out, spar, rock climb, shoot firearms, or grip anything with significant force as it can cause the muscles in your hand to apply unequal pressure to the tag and cause it to migrate under the skin. If your tag does migrate, move, or misalign during this healing process, it is not necessarily unsafe. The primary safety issue would be if the tag moved very close to any of your bones, which would increase the risk of breaking should your hand receive serious blunt force trauma that could present significant external pressure to the tag in such a way that it be caught between a bone and that external force. To date we have never had a customer report an installed tag breaking, and we've performed various physical tests our x-series tags (see durability section).

You may also experience momentary tingling, pinching sensations, or itching at the installation site for the next 12-24 months. This is normal, as it indicates your body is healing around the tag and damaged nerves around the install site are reconnecting.

Q: Does installation leave a scar?

A: Yes, but the scar is very small and typically unnoticeable after only a few months.

Q: Can the transponder be seen under the skin? Can you feel it? Is it painful or uncomfortable?

A: In most people's hands the transponder can't be seen. It will rest just under the skin without creating a visible bump, and will only show when tightly gripping large rounded objects your hand wraps around. Some people have very little fat in their fascia layer, particularly in their hands, and in certain cases the tag can be seen even when the hand is relaxed. Once the tag is fully healed in place, it's impossible to feel under the skin. It is not painful or uncomfortable, even when using your hands normally. Sometimes the thin layer of skin covering the tag will get pinched between the tag and another hard sharp surface, and you may experience a slight painful pinching sensation. For example, I would close my car door by sliding my hand across the top edge while it was closing, and this would roll the tag over that edge and it would give me that pinch feeling, so I had to change that behavior.

Q: Is it easy to remove or replace later?

A: We've designed our x-series transponders for easy removal. Unlike animal transponders, we do not coat our tags with biobond or parylene, making removal or replacement easy. Check out this blog post for more information and a video explaining the removal process.

Q: Can I install an x-series glass transponder into another area in my hand, maybe the palm side?

A: Many customers ask if it would be ok to install one of our glass transponders into another area of the hand, possibly the palm. We do not recommend that our x-series tags be installed anywhere but the suggested location between the thumb and index finger metacarpal bones. The reason for this is that the x-series tags are glass coated, meaning even though we tested them with a series of force meter tests, they should not be subjected to unnecessary stress or force. Placing a transponder in any other area of the hand will introduce additional risk, and placing one in the palm side of the hand or anywhere that exerts grip on objects, would surely result in broken glass.

Q: Can I install multiple transponders in same hand, or install one in hands with magnets?

A: It is not recommended that multiple transponders be installed into the same hand. There are interference issues and also an elevated risk of breakage. You may, however, safely install a transponder into a hand with magnets installed, as long as the magnets are not within 2 inches (5cm) of the transponder.

Q: Can I clone my work/school access card to my implant?

A: Ok, this is a big one. In short, the answer is - maybe. It all depends on the type of chip your work/school/home access card is using internally. If your source card/tag/fob is a 125kHz EM or HID Prox chip, then you can clone that ID into our xEM implant using our cloner. At this time, none of our products in the 13.56MHz frequency range can be re-programmed with new IDs.

RFID Keys
There is a common misunderstanding that somehow a "key" is programmed on to the RFID tag and in order to get access to multiple doors or systems you need to program multiple keys on to the tag. This kind of thinking is natural because that's how typical metal door keys work, but it is normally incorrect (some RFID systems do work this way but it's very rare). Each tag has a unique ID (called a UID), and these IDs are programmed into the doors and systems, not the other way around… so if you want 1000 people to get through door A, you have 1000 tag IDs programmed into door A's RFID reader. If someone loses their tag (UID 3718), they remove tag 3718 from the list and that's that. This approach means you can use one RFID tag with multiple doors and systems.

Cloning vs Emulation
Emulating means you are using a piece of active circuitry to pretend to be a tag. This basically means spoofing a reader into thinking it's talking to the spoofed tag instead of a circuit board designed to pretend to be a tag. Cloning means you copy one tag's UID and memory contents from one "source" tag's contents (ID and memory) to another "target tag" so it matches exactly. Typical tags sold by reputable companies come with the UID bits programmed by the factory and locked so they cannot be changed. This is what ensures they are unique. There are standards built on the fact that UID bits are not supposed to be changeable, meaning the manufacturers are able to keep control of the UID sequence to try to ensure uniqueness of the tags they produce. However, some chip makers have created chips that don't play by these rules, and the chips allow you to change the UID bits at will.

If you are unable to clone a tag ID to your implant, the best way to approach using your implant with school and work access control systems is to buddy up with the IT department or whoever is in charge of managing the access control systems at your work or school. Show off your implant and get them interested in seeing if it will work with the system there. Then broach the idea of trading in your access card in favor of simply adding your implant's UID to the system.

Token and Payment Systems
Now let's talk about transit and laundry cards (token systems). Typically these systems use their own method of leveraging memory blocks and access keys (Mifare Classic and DESFire access keys), meaning even if you could get your implant added to their system, it would require formatting your tag and setting up access keys in such a way that it would become totally dedicated to that purpose. You could no longer access memory blocks on your own tag or use it

for any other purpose. This might be ok for some of you, but for many I could see that as being a problem.

Now, payment systems like bank cards and credit cards. This one is really tricky because there are multiple technologies out there and they are all currently based on chips with memory structures specifically designed to make it difficult to get at the payment information stored on the card. In short, they are designed to make attempts at copying the RFID functionality to another tag difficult or impossible. Some of you may have seen articles about how easy it is to pull payment data from RFID payment cards, and these articles are telling half-truths. The reason it's easy is that the point-of-sale reader is doing the decoding work and just spitting out the payment data, but nobody has shown how it's possible to actually decode or emulate the RF interface of one of these cards.

Some people consider removing chips and antenna coils from existing transit and payment cards and implanting those, and in some cases that has occurred… but in the case of payment cards, I would not want to have to remove and replace the implant every couple years when the payment data expires. Transit systems aren't exempt from technology transitions either. Several transit systems from the Oyster system in London to my own Orca card system here in Seattle have phased out specific chip types in favor of others, sometimes multiple times. The temporary and transient nature of these systems precludes me from ever wanting to implant one of their chips into my body. There may be another solution to this problem however, so keep an eye on our Facebook page.

% **Putting xNT NFC Tag [NTAG216] After Three Months**

% **Some beginner questions regarding implants and paying**

% **RFID / NFC tags, cloning, and emulation**

% **Location / depth concerns**

% **XNT Possibilities**

2 more