eGeeTouch is a registered trademark of DIGIPAS USA LLC. They are an affiliated company of Ventura Group with a 20 year history. Located in the USA, UK, Germany and Singapore, the group company is led by Dr. Jim Li. He holds over 30 patents in the field of advanced technology deployment for electronic devices and manufacturing processes. His R&D team focuses on the development of core capabilities of advanced precision instruments and intelligent proximity access security technologies.

The intelligent proximity access in this case is in reference to a new GT2000 Smart NFC Padlock, (see photo 1). Near Field Communication, or (NFC), is a very new technology related to the locksmith industry. NFC devices have extremely low power consumption. The lock is powered by two, A76/LR44 1.5V button batteries that will last for two years at five openings per day.

The eGeeTouch® is the world’s first patented NFC-driven smart electronic padlock. The advantages of this smartlock are:

1. It needs no mechanical key.
2. It enables loss tags or paired smartdevice’s IDs to be denied/deleted only by authorized lock’s owner using eGeeTouch App without the need to change the entire padlock or cylinder.
3. It is capable of tracking unlocking records on WHO, WHEN & WHERE an access was made providing an audit trail (audit log) - a security-relevant chronological record, containing documentary evidence of the sequence of access history which is a highly useful new feature unmatched by any conventional mechanical padlock.

First, let me tell you a little about Near Field Communication (NFC).

Near field communication, or “NFC” for short, is an offshoot of radio-frequency identification “RFID”. NFC is designed for use by devices within close proximity to each other. This means very close.

Bluetooth and Wi-Fi seem similar to near field communication on the surface. All three allow wireless communication and data exchange between digital devices like smart phones for example. However, near field communication utilizes electromagnetic radio fields, while technologies such as Bluetooth and Wi-Fi focus on radio transmissions instead.

Devices using NFC may be active or passive. A passive device, such as an NFC tag, contains information that other devices can read, but does not read any information itself, (see photo 2). Think of a passive…
device as a sign on a wall. Others can read the information, but the sign itself does nothing except transmit the information to authorized devices.

Active devices can read information and send it. An active NFC device, like a smartphone, would not only be able to collect information from NFC tags, but it would also be able to exchange information with other compatible phones or devices and could even alter the information on the NFC tag if authorized to make such changes.

NFC works using magnetic induction, (see photo 3). The reader emits a small electric current which creates a magnetic field that in turn bridges the physical space between the devices. That field is received by a similar coil in the client device “in this case a lock,” where it is turned back into electrical impulses to communicate data such as identification number status information, or any other information. So-called ‘passive’ NFC tags use the energy from the reader to encode their response, while ‘active’ or ‘peer-to-peer’ tags have their own power source and respond to the reader using their own electromagnetic fields.

Like RFID, NFC works in the 13.56MHz radiofrequency spectrum using less than 15mA of power to communicate data over distances that are usually less than 10cm, or four inches. Tags typically store between 96 and 512 bytes of data and transfer data at speeds of 106Kb/s, 212Kb/s, 424Kb/s, or 848Kb/s, enough to move small pieces of information virtually instantaneously as is essential in high-volume transport applications.

So for those that are worried about NFC, let’s look at the most common question. How will I be able to stop people from taking my information if all they have to do is stand next to me?

The thing about NFC is that it is safe in a couple of ways. First of all, your phone does have to be within a few centimeters of another phone for the information to be transferred. Not only that, but you both have to give permission to send and receive information. To ensure security, NFC often establishes a secure channel and uses encryption when sending sensitive information such as credit card numbers. So there is no way for your information to be unwittingly shared.

The benefits of using eGeeTouch® proprietary proximity-access NFC technology over Bluetooth-enabled lock are:

1. Higher security, eradicating concerns over any unwanted vicinity interception or hijacking Over-The-Air (OTA) transmissions that Bluetooth locks expose to.

2. Faster connection speed that require very short, typically less than a second access time.

3. Negligible power consumption as NFC tag is a passive device thus extending battery life to years.

An eGeeTouch® NFC tag or NFC-paired smart devices such as NFC-enabled Android Smartphone or NFC-sticker tagged in wallet, offer significant choices to accommodate diverse user’s preferences as alternatives for
multiple access methods for unlocking.

Now back to the padlock.

We have already talked about the batteries used to power the lock. To replace the batteries is simple. Remove the cover screw using a #0 Philips head screwdriver, (see photo 4). Remove the cover, (see photo 5). Now pull out the battery holder to replace the batteries, (see photo 6). Simple as that!

One very nice thing about NFC devices is their ability to work with NFC Fobs, NFC tag stickers, or a NFC compatible smart phone, (see photo 7). That's right, just wave your phone over the lock and it will open if the lock has been programmed to accept your phone.

How safe is this. Very! The state of the art NFC proximity access security, proprietary encryption, and smart identification technologies generate over 100 million encrypted IDs. There is even an audit trail inside the lock. It looks like high tech padlocks are here.

I love to take things apart. So guess what we are going to do now? We are about to dive inside the GT2000 to see what makes this padlock work.

To start with, I tried drilling the three cover attachment points to remove the cover, (see photo 8). After drilling however, I was unable to pry off the cover. So we move on to more destructive measures. I used a 1” end mill to cut my way down into the lock, (see photo 9). This worked great and was a lot of fun as well!

The end result of the work with the end mill was that the cover fell off and exposed all of the goodies inside, (see photo 10). The black part in the middle is a solenoid. The solenoid, being spring loaded, will push up between the locking pins for the shackle and prevent the lock from opening, (see photo 11). When the solenoid receives power, the plunger is retracted and the locking pins will slide inward when pressure is put on the shackle. Here is another look at the removed solenoid, (see photo 12).

With the solenoid removed, you can see the electronic circuit board that controls everything, (see photo 13). This is the other side of the board, (see photo 14). I was curious if the board had been covered with a protective coating to prevent moisture from shorting the electronics, so I looked at the board under
a microscope at 16X. I used a needle to scrape across the board and saw a plastic type coating being removed by the needle. So the board is in fact coated to prevent moisture from causing a problem. However, if this lock was exposed to salt water, or salt water environment, I feel fairly certain that over time it would corrode the internal workings of this lock.

The last thing I want to show you is the antenna used to emit the magnetic field as well as receive the transmitted signal from the NFC tag, (see photo 15). All of the circular pattern on the circuit board is part of the antenna. This is some really cool stuff, don’t you think? Here are some of the features of this lock.

- Ultra high security because of the NFC technology.
- Audit trails.
- Multiple access methods which include smart phones and NFC Fobs.
- Splash proof and freeze proof due to their resistance to water and extreme temperatures. -10C to +50C.
- Backup power through USB 2.0 connectivity.
- LED and buzzer notification.
- Shackle clearance is 33mm by 35mm.
- Shock proof to 1.5 meters.

With eGeeTouch® smarter padlock, unlocking a gate/door becomes a seamless act. All actions are accountable with a traceable access history for safeguarding your personal belongings in the locker, gate, indoor storage or cabinet. No more lost keys, replacing cylinders or duplicating mechanical keys, forgetting codes. Since there is no mechanical key hole in a smartlock, there is no worry about vulnerabilities associated with key picking or key bumping. Simply press the shackle lightly to ‘wakeup’ the smart lock, follow by tapping a NFC-paired smartphone or tag to front-face of the lock to unlock.

eGeeTouch also make a Smart Luggage Lock, and a Smart Travel Padlock with the same NFC capabilities.

So whether you use a smart phone or a NFC tag, the future of this product and its technology is definitely going to expand.

For more information contact:
DIGIPAS USA LLC
304 W Main Street, #120
Avon, CT 06001
Phone: (1) 860 373 9634
Website: www.digipas.com