Why risk it?

Protect your reputation with genuine NXP MIFARE products

By Markus Luidolt, NXP Semiconductors

Abstract

Fake MIFARE products, including counterfeit ICs and cloned smartcards, pose a significant risk to everyone involved, from manufacturers and suppliers to retailers and consumers. Insisting on genuine MIFARE products, available from a wide global network of authorized partners, provides all the benefits of ensured quality, reliability, performance, and interoperability, while fostering end-user confidence. Using the latest MIFARE products helps reduce risk even more, since they deliver state-of-the-art security and support for NXP's Originality Checker, which lets anyone verify the authenticity of a card IC.

In today's global economy, supply chains often involve a complex network of third-party companies operating in different regions. Internationalization, outsourcing, e-retailing, and other activities make it harder to control the process and create opportunities for unauthorized and counterfeit products to contaminate the original supply. High-priced luxury goods like handbags and watches may be the first things that come to mind when the topic of product counterfeiting pops up. But the reality is that unauthorized, non-licensed, and non-certified products are an increasingly widespread issue in just about every market.

MIFARE-based smartcards, for example, which are used by hundreds of millions of people every day in applications such as ticketing, access, and micropayment, have also become targets for counterfeiters, black-market suppliers, identity thieves, and other criminals hoping to gain from MIFARE's increasing popularity. As a result, unauthorized card components and cloned cards have found their way into the market, where they are bought by unsuspecting customers.

This paper discusses the benefits of using only genuine NXP MIFARE products, and explains how manufacturers, suppliers, retailers, and service providers can protect themselves from incurring the losses associated with fakes and forgeries.

We begin with a look at why imitators are drawn to the MIFARE brand.

Follow the leader

MIFARE, which is the world's leading application development platform for contactless smartcards, smartphones, wristbands, and other form factors, has been growing in popularity since it was first put to use in the mid-1990s. In total, more than 1.2 billion people have access to MIFARE-based systems every day in over 70 countries.

MIFARE is the basis for dozens of applications, including closed-loop payment cards, employee badges, student IDs, transport tickets, hotel keys, and access passes. More than 150 million MIFARE reader ICs, along with more than ten billion card components, have been sold to date. The huge installed base of MIFARE products makes it easy for service providers to expand their offerings while reducing overall costs and increasing user convenience. Widespread availability, ease-of-use, transaction speed, and reliability have all contributed to the longevity and continued success of NXP's MIFARE technology.

MIFARE has a typical operating distance of up to 10 cm (4 inches), and offers very fast transaction times – a typical ticket transaction takes less than 100 ms. MIFARE supports multi-application use cases, so that a single smartcard can be used with multiple services. On top of this, the most recent versions of MIFARE have earned high security ratings as defined by ISO/IEC 15408, the Common Criteria for Information Technology Security Evaluation (www.commoncriteriaportal.org).

The following statistics serve to underpin just how successful MIFARE is:

- Used in more than 736 cities worldwide
- More than 40 different application categories
- More than 77% of all automatic fare collection (AFC) schemes
- More than 80% of all contactless, limited-use ticketing credentials
- More than 55% of all high-frequency (HF) access-management systems
- More than 150 million readers and 10 billion card components shipped

Success has a way of breeding imitation, especially when there is a chance for monetary gain. As with any technology that supports payment transactions, secure access, or a combination of the two, MIFARE is a target for black-market operators and other criminals hoping to profit from the use of imitation products.

Risky business: liability and loss

There are two main reasons why using unauthorized or counterfeit MIFARE products is a risky business. The first is liability, and the second is loss of customers. Both have the potential to be very costly to a company.

Legal liability

NXP Semiconductors is the sole owner of the technology related to MIFARE products, all MIFARE trademarks, and all the intellectual property rights (IPR) relating to MIFARE. Anyone caught using or selling counterfeit MIFARE products can be found liable for damages.

The laws governing IPR prohibit manufacturers from manufacturing unlicensed products, but also make it illegal for OEMs and traders to import, sell, or

otherwise dispose of products that include IPR-infringing components. The unauthorized use of trademarks is also a criminal offense. Even the advertising of such products may be prohibited. Counterfeit products can be subject to seizure by customs authorities, and courts can ban them from the market. Public disclosure of these criminal acts can seriously impact a company's reputation in the client community, and can do irreparable damage to a company's products and services.

NXP is fully committed to taking any necessary action to protect its rights and does not tolerate infringements. Our zero-tolerance policy means that we actively pursue any and all IPR infringements. Our legal department and our MIFARE Intellectual Property Protection Team are actively working on hundreds of cases. These legal actions have already led to remarkable results, including the following:

- More than 60,000 unauthorized MIFARE products on auctions, webshops, and web pages have been taken off the market, preventing their sale and resulting in losses for their vendors.
- Ongoing activities have temporarily halted or permanently shut down a large number of black-market dealers.
- Dozens of individual cases involving the use of fake products have successfully been converted to genuine MIFARE products, including loyalty cards in Australia, university cards in the United Kingdom, and food-court cards in Asia, among many others.

NXP has teamed up with REACT, a member-based anti-counterfeiting network **(www.react.org)**, to uncover companies that offer MIFARE clones and infringe IP rights. This partnership has triggered successful seizures of unauthorized MIFARE products at exhibitions in Europe as well as in Hong Kong, China.

The seizures removed all fake products, promotional material, and booth elements relating to MIFARE, and initiated lawsuits. News coverage of these activities is available at **www.react.org/news-a-events/item/567-mifare**.

NXP encourages anyone who discovers unauthorized or counterfeit MIFARE products to report their findings to NXP by emailing **MIFARE@nxp.com**.

In light of NXP's dedication to protecting its MIFARE brand, companies can be certain that NXP will take action if they are found to be promoting or selling unauthorized or counterfeit MIFARE products.

Loss of customers

Another risk, beyond legal liability, is the fact that unauthorized copies of MIFARE might not meet basic requirements and therefore might create problems that negatively impact performance and security, and ultimately drive customers away. Here are some examples:

- **More field returns** – Unauthorized copies of MIFARE often fall short in terms of quality, and can result in higher rates of field returns and non-working products. This can increase customer-service costs, damage end-customer confidence, and impact the service provider's reputation.

- **Interoperability issues –** Unauthorized copies may not meet the requirements of ISO/IEC standards, and this can impact interoperability. System components and credentials may not be secured properly, and may not match the formats used by different generations of MIFARE readers, causing problems when consumers try to use the card.

- **UIDs that can't be trusted** – A cloned card may have had its unique identifier (UID) modified, and that means the UID may not be trustworthy. This can impact the supply chain, since UIDs are part of the inventory-tracking process, and can compromise user accounts, since it may not be possible to match the right owner with the right card.

- **Faulty security algorithms** – The most recent generations of MIFARE ICs use Common Criteria certification from accredited authorities to ensure the highest levels of data security. Counterfeit cards don't use these certifications, and this places personal user data at risk of being hacked or cloned. This is because, without Common Criteria certification, a counterfeit product that adheres to specifications and operates properly is still vulnerable to attack, since criminals can track the unprotected chip's behavior or access its data. Obtaining Common Criteria certification is not easy. Producing an IC that is resistant to different attack scenarios is expensive, in terms of R&D and production, and there is the added cost of verifying resistance to obtain certification. In many cases, counterfeit products are cheaper because they skip these steps.

- **Complex migration** – Authentic MIFARE products are designed for seamless migration to next-generation functionality, but counterfeit ICs may not be. When it comes time to upgrade a system based on counterfeit ICs, the process may be more complex than necessary, with higher costs and a more intense development effort.

Performance issues like these can increase operating costs, disrupt business continuity, damage the brand, and erode customer satisfaction.

Reduce risk: use genuine MIFARE products

The good news is that there are several ways that manufacturers, suppliers, retailers, and even consumers can reduce these risks. Genuine NXP MIFARE products deliver the security, interoperability, and reliability required by today's contactless systems. By insisting on genuine MIFARE products, everyone can be sure they're working with technology they can trust.

The latest generations of genuine MIFARE products are the only ones that can be guaranteed to offer all of the following:

- Strict compliance with the ISO/IEC 14443 standard
- Common Criteria certification for security (except for MIFARE Classic and MIFARE Ultralight)
- Full compliance with NXP's stringent standards for quality
- High-volume production in state-of-the-art wafer fabs
- Benchmark global support services
- Seamless migration to newer generations

NXP's commitment to MIFARE has created a best-in-class technology backed by an extensive ecosystem that ensures highest quality. The widespread success of MIFARE is linked to NXP's strategy for extending and protecting the brand, going beyond legal actions to create a thriving community of partners, developers, and consumers.

Licensing and certification

Although NXP is the sole owner of the MIFARE brand, NXP has developed a global network of third-party companies and business partners who support MIFARE's success. NXP has granted technology licenses to semiconductor and card manufacturers around the globe, so smartcard suppliers have a wide range of options for genuine MIFARE products.

The MIFARE community, which is the largest network of companies involved in contactless system solutions, plays an important role when it comes to educating the market about the risks of unauthorized products.

In addition, NXP has developed relationships with two independent test houses, Arsenal and UL, to verify and certify the functionality and interoperability of MIFARE-based systems. Having a worldwide certification program in place contributes substantially to the strength and dependability of the MIFARE brand. More about these two organizations, and details on the certification process, can be found at www.mifare.net/en/aboutmifare/mifare-certification.

Recommended suppliers

NXP-recommended suppliers, which include MIFARE Premium Partners, are professional organizations that offer genuine MIFARE products. The most current list can be found on www.MIFARE.net, under the tab "Companies".
When considering a MIFARE purchase, if it's not clear that the supplier has been approved by NXP, think carefully before buying. If something looks off, it probably is. Take into account where and how the item is being offered. If you're buying online, does the website have any contact information? Is the product sold in a professional package? Are there noticeable errors in text or grammar? Is the price dramatically lower than you've seen elsewhere? If the store, the package, or the price seem questionable, then the product on offer is less likely to be authentic.

Verification tools and services

NXP is committed to helping developers, suppliers, and consumers verify the authenticity of genuine MIFARE smartcards, and has developed a series of tools and services that make it possible to verify authenticity at any point in the product lifecycle.

- **IC selection** – The best way to ensure authenticity is to buy from an NXP-recommended supplier. The partner list that appears on the "Companies" tab of www.MIFARE.net is a good place to start. In extreme cases, if there are doubts about an IC's origins, the NXP lab in Austria can perform a physical analysis.

- **During development** – Using the MIFARE Software Development Kit (SDK) helps designers take full advantage of authentic MIFARE performance. It also ensures that any Android app developed for use with the card works as promised.

- **Post production** – Once cards have been released for production, a desktop system with a built-in card reader, called the NXP Originality Checker, can be used in the supply chain to verify a card's origins before adding it to inventory or offering it for sale.

- **On the open market –**The latest MIFARE ICs support a feature, called NXP Originality Check. This feature, which works with TagInfo, a free NXP Android app, lets anyone, including consumers, check authenticity before buying or using a MIFARE-based contactless smartcard.

Details on these NXP tools and services can be obtained by emailing MIFARE@nxp.com.

A special case: MIFARE Classic

While genuine MIFARE products are always a better choice than unauthorized or counterfeit versions, it's important to note that there is a case where even using genuine MIFARE technology can expose a too high vulnerability. In systems that continue to use MIFARE Classic, the original version of MIFARE introduced in 1994, operators are vulnerable – even if they are using genuine MIFARE Classic products – because MIFARE Classic is less secure than more recent generations of the MIFARE product family. Backward compatibility means that cards based on MIFARE Classic work seamlessly in today's updated infrastructure, but we discourage operators from continuing to use MIFARE Classic, due to the technology's security concerns.

MIFARE Classic has had a remarkable run – it's hard to find other technologies from the mid-1990s that are still as widely used today – but the years are starting to show. By almost any technology standard, MIFARE Classic is ready for retirement.

Known vulnerabilities

In 2007, the proprietary crypto algorithm used in MIFARE Classic was shown to have flaws and weaknesses. Various third parties, including university researchers, revealed vulnerabilities in MIFARE Classic that limit its use in secure environments.

Researchers at the University of Virginia demonstrated that, with cards based on MIFARE Classic, one could clone a ticket or change its value to gain illegal access to the service provided. Similar cloning and tampering scenarios are possible with other applications, such as hotel key cards, and electronic payment schemes.

Contactless smartcards usually have a separate area of memory for storing extra information, such as the dollar value of a ticket used in a public-transport system. In cards based on MIFARE Classic, the memory uses weak or outdated encryption algorithms, so the memory can be hacked and the data can be stolen or changed. Reverse-engineering efforts have shown that MIFARE Classic may allow hackers to alter the card's memory and access user data. Taking the next step, and programming the UID and the hacked data and keys into counterfeit products, makes it possible to replicate a card, and to create forged copies for illicit use or sale on the black market.

Here's an example of what this might mean in a real-world application, such as a car-sharing service. Members use a smartcard to unlock the vehicle and pay for the rental. With MIFARE Classic, counterfeiters could forge a card and use it to access the car illegally. Or, using a valid card, the vehicle could be taken to a garage where forgers, using equipment readily available online, could hack the keys and create an unlimited number of new cards for unauthorized sale. The widespread use of payment cards and access passes makes this kind of vulnerability a serious issue.

MIFARE Classic EV1 is an improvement

Uncovering these flaws prompted NXP to re-evaluate its approach. The MIFARE Classic EV1 versions are hardened against „card-only" attacks as full key diversification (every card having different keys) is used They are less susceptible to hacking than the original MIFARE Classic. Card-only attacks are attacks where the adversary only needs to have access to a card. For other attacks they need to have access to the readers in the operational system, where they run a higher risk of being detected.

MIFARE Classic EV1 versions also offer upgraded performance and more reliable assembly. They also carry the NXP Originality Signature, which makes it easier to authenticate genuine products. Migrating to MIFARE Classic EV1 lets the system take advantage of NXP's heavy investment in R&D, for higher performance and improved asset protection, without adding costs. MIFARE Classic EV1 versions sell for the same price as MIFARE Classic versions, and there is no need to change the existing infrastructure to implement the upgrade.

It's important to point out, though, that some of the vulnerabilities of MIFARE Classic remain in place even if cards are upgraded to MIFARE Classic EV1. This is because the problem cannot be solved in the card alone. For state-of-the-art security, we recommend upgrading the cards and the infrastructure, moving to systems that use the MIFARE Plus or MIFARE DESFire formats.

MIFARE PLUS and MIFARE DESFire are the most secure options

For applications where security is key, like closed-loop payment, access management to secure sites, or automatic fare collection systems in public transport, we recommend using MIFARE PLUS and MIFARE DESFire.

MIFARE Plus offers a unique way to upgrade systems that use MIFARE Classic to a scheme based on advanced AES-128 security. The functionality of MIFARE Plus is compatible with MIFARE Classic, and supports migration to the AES scheme while maintaining application data. The infrastructure upgrade can be done gradually, before cards are switched in the field. A major advantage is that cards based on MIFARE Plus can be deployed before the infrastructure is migrated to AES, thus speeding up the replacement of legacy and vulnerable cards.

MIFARE DESFire uses a highly secure and flexible architecture to deliver the features required by state-of-the-art contactless systems. Across a number of application categories, systems based on MIFARE Classic are being migrated to MIFARE DESFire. In installations that have a large number of active cards, both types of cards – MIFARE Classic and MIFARE DESFire – can run in parallel for a time, even after the contactless readers have been upgraded. The readers choose the correct functionality based on the card's identification parameter.

Conclusions

NXP's MIFARE products are the world's choice for contactless smartcards, and NXP works hard to protect the integrity of its MIFARE brand. Unfortunately, the success of MIFARE makes it a target for black-market suppliers and other criminals, and counterfeit components and cloned cards do, on occasion, find their way into the marketplace.

Fake MIFARE products pose a significant risk and can lead to lost revenue, security breaches, legal problems, and loss of customer faith. The better choice is to avoid these risks and use genuine MIFARE products only sold via recommended NXP partners. Genuine products provide all the benefits of performance, interoperability, and seamless upgradability, and help ensure customer satisfaction.

NXP advises phasing out MIFARE Classic, which has had known security risks for several years. Transitioning to newer versions of MIFARE products is straightforward and cost-effective, and can serve to increase security and minimize risk. The latest generations of MIFARE offer higher levels of security, so they are harder to attack, hack, or clone, and are supported by NXP's Originality Checker, the desktop and smartphone app that lets anyone verify MIFARE authenticity.

www.nxp.com

Date of release: December 2014
Document order number: 9397 750 17626
Printed in the Netherlands