Keywords: counterfeiting, anti-counterfeiting, brand protection, authentication, strong authentication, challenge-response authentication, RFID, SHA, SHA-1, SHA-2, iButton, secure memory, tag, knock-off, cloning, anti-cloning, near field communication

APPLICATION NOTE 5416

# Ubiquity of NFC-Enabled Phones Leads to Strong Brand Protection

By: Hamed Sanogo, Executive Business Manager, Secure Info & Authentication
Christophe Tremlet, Security Segment Manager
Mar 06, 2013

*Abstract: Counterfeiting has grown tremendously over the last decade. Fortunately, there are several anticounterfeiting solutions. Of these, an authentication based on challenge-response allows a much stronger protection than secure printing or unique ID RF tags. This application note presents the benefits of RFID tags based on crypto-strong authentication. It explains how these benefits enable the consumer to check for the authenticity of luxury goods by simply tapping their near-field communication (NFC)-enabled phones.*

A similar version of this article appeared in German on *Elektronik Praxis*, August 13, 2012.

## Introduction

Counterfeiting has grown tremendously over the last decade. According to government data, officials seized $188 million worth of counterfeited merchandise in the U.S. in 2010. Not only is the overall value of counterfeited goods increasing, but counterfeiting is penetrating more and more sectors. Among these, luxury goods are a target of choice, as their value heavily relies on the brand itself. Obviously, due to the cost of luxury items, the incentive for counterfeiters is high. Counterfeiting has an impact on the brand owner, as it creates revenue loss; but even worse, it damages the image of the brand. The consumer is also a victim, especially when there is no way to check whether a luxury-branded item is genuine.

There are several anticounterfeiting solutions. Of these, advanced printing techniques are still the most prevalent, which include holograms, unique ID numbers, and tamper-proof labels. To answer the increasing level of threats, some companies have also adopted RFID technology, where an RFID tag is attached to the item to be protected. At any moment, the tag can be checked through an appropriate reader. If the data read from the tag matches with the expected data, the item is authenticated and recognized as genuine.

## Risks, Drawbacks, and Weaknesses of a UID-Based Solution

Most RFID solutions deployed today are based on a unique serial number or "UID." The core principle of UID-based solutions is that each tag contains a unique number. When read from the RFID tag, this number is checked by the authentication system against its records. If the number is part of the database, it is considered a valid number and the good is authenticated. This provides a first level of protection, but the weakness of such systems is that they are sensitive to man-in-the-middle (MITM) attacks. With an off-the-shelf reader, an attacker can intercept a serial number and record it. Once the number is recorded, the attacker can easily forge a fake tag. The same serial number is programmed in a new off-the-shelf tag, and the tag is cloned for reuse. System integrators have implemented countermeasures to mitigate these kinds of attacks. For instance, the reading infrastructure might check if a given number has already been used or if the geographic location matches the one expected.

While these countermeasures are effective, they have two drawbacks: they increase the complexity of the infrastructure, and they do not allow the end customer to check that the good is genuine. An advanced infrastructure can be deployed in warehouses, but one can hardly imagine it installed at a final retailer. Furthermore, it is desirable for buyers to be able to independently identify fake objects. Considering the fact that security is at least partly implemented in the infrastructure, this seems hardly achievable.

We will see how challenge-response-based tags can allow buyers to detect counterfeited goods themselves thanks to near-field communication (NFC) technology, thus overcoming the current limitations of the UID-based tag technology.

## Description of the Challenge-Response Principle

In its simple form, the challenge-response principle, also known as challenge-response authentication, is a hand-shaking protocol in which one party (the NFC phone) presents a question ("challenge"), and another party (the NFC tag) must provide a valid answer ("response") to be authenticated. Using challenge-response to identify a friend or foe status of connecting devices has been in practice in the wired world for years. It is commonly used in printer cartridge and medical consumables, notebook computer battery packs, and power adapters.

With the NFC-based challenge-response authentication principle, anyone will be able to use an NFC-enabled cellular phone to scan a luxury good to check for authenticity. Manufacturers would only need to hide a SHA-1-based NFC tag on the luxury good (e.g., embed a tag IC in the cork of the rare wine bottle). The NFC reader will then be able to identify the item as genuine after it has been authenticated as such.

The major components of an NFC authentication scheme include the **random challenge**, the **tag's UID**, and the **secret**. The secret is programmed in the tag's protected memory and is known by the cellular phone's application software API. A strong key management is required to keep the system from being compromised.

As shown in **Figure 1**, when the NFC-based cellular phone comes near the vicinity of the luxury good equipped with a SHA-1-enabled tag, the following sequences of events take place:

- A near electromagnetic field establishes between the phone and the item.
- The electromagnetic field energizes and wakes up the tag.

- The handset establishes a connection with the tag via ISO 14443/15693 protocol.
- The handset reads out the tag's UID.
- The handset's API generates a random challenge and sends it to the tag. The tag computes a SHA-1 message authentication code (MAC) with its UID, secret, and the random challenge received.
- The handset locally computes its own MAC with its locally stored secret, random challenge (the same one which was sent to the tag), and the UID read from the tag.
- Handset compares the value of its MAC against the one computed by the tag.
- If the two MACs match, the tag is authenticated. The handset might then read additional data from the tag's memory, such as the date and place of manufacture and the lot number. This essentially means that the product is genuine. However if the MACs do not match, the item is deemed fake, a knockoff, or counterfeit.

Figure 1 visually summarizes the challenge-response authentication principle.

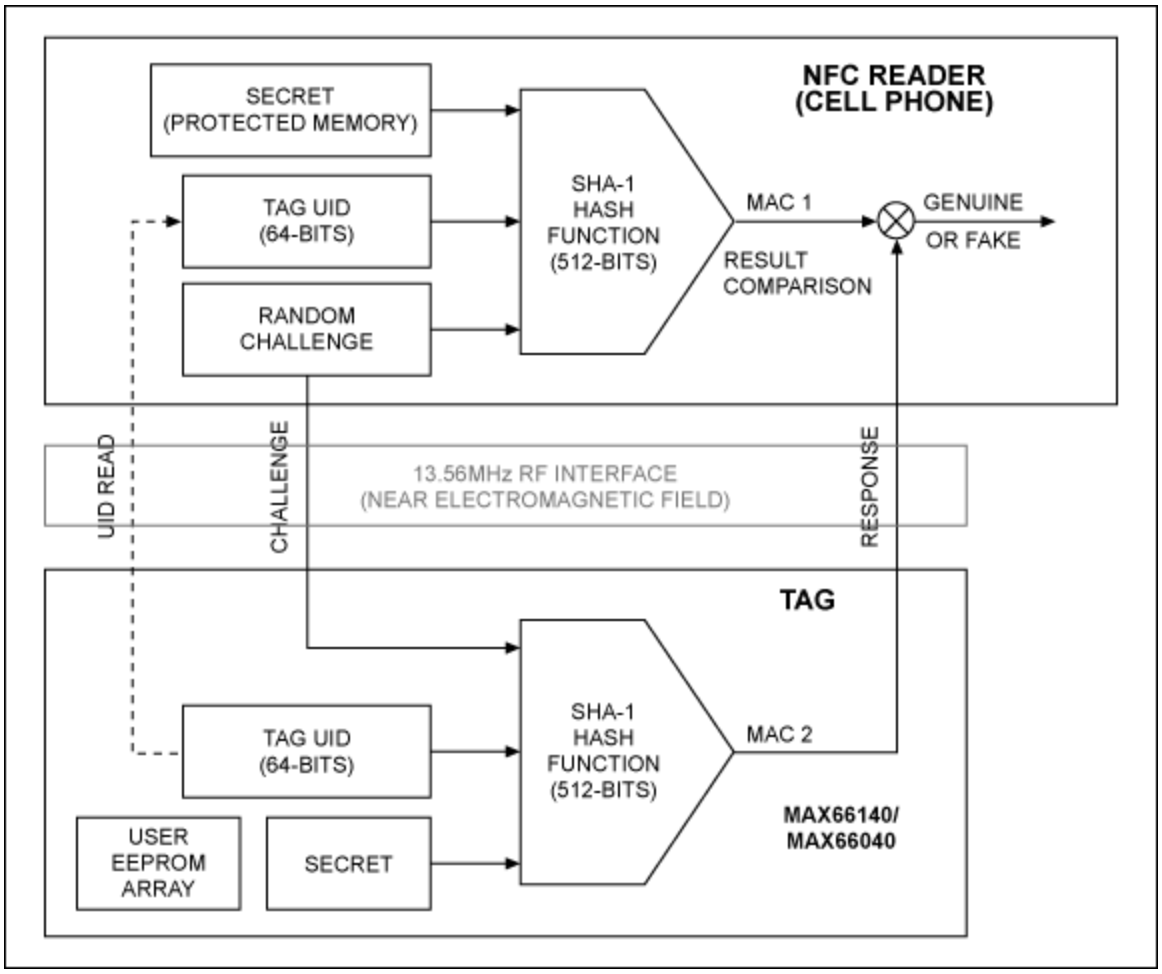


*Figure 1. SHA-1-based challenge-response authentication principle.*

## Benefits of the Challenge-Response

While manufacturers have been relatively successful in eliminating electronic device counterfeits (mainly

because they have power and electronics circuits on board in applications where contact is made), this success has not been seen with cloned apparels, medicines/drugs, designer handbags, shoes and sunglasses, as well as with knock-off perfume and wine bottles, just to name a few. The lack of a proper solution to the counterfeit epidemic has led to a continuously growing market for counterfeits, replicas, and imitation goods, which most likely do not meet the manufacturing standard or the safety and protection provided by their genuine counterparts.

A strong crypto hash technology like SHA-1, combined with NFC technology, makes a strong anti-counterfeiting/cloning tool. It is nonreversible (as it is computationally infeasible to determine the input corresponding to a MAC), collision-resistant (since it is impractical to find more than one input message that produces a given MAC), and has a high avalanche effect (as any change in input produces significant change in MAC result).

Buying a luxury good with peace in mind can become an easy endeavor. Just a slight scan over the items and the user knows within a few seconds whether the object is genuine. Another key benefit of this technology is the elimination of counterfeit drugs and perfumes/fragrances, which can be very hazardous to public health. These types of counterfeits have an additional negative impact on manufacturers in terms of sales revenue and a customer loyalty decline, due to imitations that do not produce the authentic products' claimed effects. In addition to enabling product authentication by end customers, challenge-response authentication also dramatically simplifies the RFID infrastructure for both the manufacturer and the supply chain. This is especially a relief for the latter; because of UID RFID weaknesses, the supply chain has had to implement countermeasures in its infrastructure. This included combining the UID with a geographical location, checking that a number is not used twice, and so on. As opposed to UID-based solutions, in challenge-response-based implementations, security is self-contained in the tag-enabling product's authenticity verification. This is accomplished with a simple, lightweight reader that does not need to be sustained by a sophisticated infrastructure.

Maxim's MAX66140/MAX66040 solution combines 1024 bits of user EEPROM, 128 bits of user and control registers, a 64-bit UID, one 64-bit secret, a 512-bit SHA-1 engine, and a 13.56MHz ISO 14443B/15693 RF interface. These ICs come in a variety of packaging, including key fob, inlays, ISO cards, wound coil, bare die, and custom packaging. The strength of the MAX66140/MAX66040 tag in combating counterfeiting resides in the size of the SHA-1 engine (512 bits), the cost, and SHA-1 engine's fast computation time. Maxim also provides the means to achieve an effective key management.

The secure 1-Wire® SHA-1-based products have been used in both the printer and medical consumables markets for many years. To date, over 300 million units of Maxim's proven solutions have been sold. These devices have been designed to prevent against both physical and side-channel attacks. The MAX66140/MAX66040 come from that line of products.

## Conclusion

With the ubiquity of NFC-enabled cellular phones and the boost that this has added to the NFC ecosystem, an imminent anticloning solution has just been created. By hiding a SHA-1-enabled tag on their products, and by making APIs and software applications available to all cellular phone users, manufacturers can get end users to help protect their brands against counterfeits. Essentially, someone who buys a counterfeit item can be discovered quickly. The potential opportunity for embarrassment in purchasing a knock-off item may also help impede the growth of the counterfeiting market.

1-Wire is a registered trademark of Maxim Integrated Products, Inc.

| Related Parts | | |
|---|---|---|
| MAX66040 | ISO/IEC 14443 Type B-Compliant Secure Memory | Free Samples |
| MAX66140 | ISO 15693-Compliant Secure Memory | Free Samples |

**More Information**
For Technical Support: http://www.maximintegrated.com/support
For Samples: http://www.maximintegrated.com/samples
Other Questions and Comments: http://www.maximintegrated.com/contact

Application Note 5416: http://www.maximintegrated.com/an5416
APPLICATION NOTE 5416, AN5416, AN 5416, APP5416, Appnote5416, Appnote 5416