# SECURE SYMMETRIC AUTHENTICATION FOR RFID TAGS


## Abstract:

The growing use of Radio Frequency Identification (RFID) technology to enhance ubiquitous computing environments has only begun to be realized. It allows for the identification of objects and/or subjects remotely using attached RFID tags via a radio frequency channel, hence identification is achieved in a contact less manner. The advantages of using RFID technology is growing tremendously and is gaining much attention as is seen by an increase in its deployment, such as object tracking and monitoring, supply-chain management, and personalized information services. Numerous authentication protocols for RFID systems were proposed in an attempt to prevent unauthorized tracking and monitoring, impersonation or cloning, and information leakage. Many of these attempts fail to enforce anonymity and order only weak authentication and some fail under denial of service.

With a small introduction to RFID tags this paper enhances passive RFID (Radio Frequency Identification) tags with cryptographically secure authentication. Starting with a short introduction into common RFID systems, we present a motivation why secure authentication with standardized symmetric crypto algorithms for RFID tags is necessary for many applications. We demonstrate vulnerabilities of current RFID systems and explain how application of an authentication mechanism can solve them. Furthermore we explain how authentication protocols work and how they can be included in the RFID protocol standard ISO 18000. By presenting the interim results of ART, we will show that the proposed enhancement is feasible with current RIFD infrastructure and silicon technology used for RFID tags.



**Key Words:** *Radio Frequency, Monitoring, Rfid Tags, Authentication.*


**Conclusion:** In this paper we started with a short introduction to current RFID systems. We showed how the basic principles work and we motivated the enhancement of actual RFID systems with authentication functionality with standardized methods and algorithms. The main result so far is that we showed, that secure symmetric authentication is feasible for current RFID technology without significant additional costs. RFID with authentication is not only necessary to use RFID technology in security relevant applications but also if the tags contain personal data.

Its important to realize that there will be no universally “Right” solution even for similar application with in the same industry .Every RFID solution each company adopts will be unique.

## INTRODUCTION

Radio Frequency Identification (RFID) is an emerging technology. The main idea behind it is to attach a so called RFID tag to every object in a particular environment and give a digital identity to all these objects. An RFID system is an small portable computer without a screen and a keyboard that interacts with the world through radio frequency signals. An RFID tag is a small microchip, with an antenna, holding a unique ID and other information which can be sent over radio frequency. The information can be automatically read and registered by RFID readers. The data received by the RFID reader can be subsequently processed by a back-end database.

## RFID SYSTEM

The tag contains a transponder with a digital memory chip that is given a unique electronic product code. The interrogator, an antenna packaged with a transceiver and decoder, emits a signal activating the RFID tag so it can read and write data to it. When an RFID tag passes through the electromagnetic zone, it detects the reader's activation signal. The reader decodes the data encoded in the tag's integrated circuit (silicon chip) and the data is passed to the host computer. The application software on the host processes the data, often employing Physical Markup Language(PML).

A basic RFID system consist of three components:

1. An antenna or coil
2. A transceiver (with decoder)
3. A transponder (RF tag) electronically programmed with unique information

Figure 1 gives a graphical overview of an RFID system.

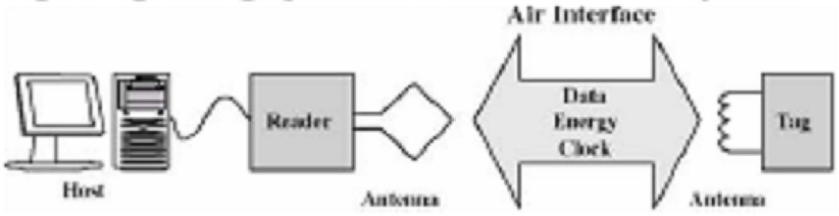


Figure 1: Overview of an RFID system.

The antenna emits radio signals to activate the tag and read and write data to it. Antennas are the conduits between the tag and the transceiver, which controls the system's data acquisition and communication. Antennas are available in a variety of shapes and sizes; they can be built into a door frame to receive tag data from persons or things passing through the door, or mounted on an interstate toll booth to monitor traffic passing by on a freeway. The electromagnetic field produced by an antenna can be constantly present when multiple tags are expected continually. If constant interrogation is not required, the field can be activated by a sensor device. Often the antenna is packaged with the transceiver and decoder to become a reader (a.k.a. interrogator), which can be configured either as a handheld or a fixed-mount device. The reader emits radio waves in ranges of anywhere from one inch to 100 feet or more, depending upon its power output and the radio frequency used. When an RFID tag passes through the electromagnetic zone, it detects the reader's activation signal. The reader decodes the data encoded in the tag's integrated circuit (silicon chip) and the data is passed to the host computer for processing.

## TYPES OF RFID TAGS

The RFID tags are again classified into three types.They are

1.Active
2.Semi passive(=semi active)
3.Passive

Passive RFID tags have no internal power supply. The minute electrical current induced in the antenna by the incoming radio frequency signal provides just enough power for the CMOS integrated circuit (IC) in the tag to power up and transmit a response. Most passive tags signal by backscattering the carrier signal from the reader. This means that the aerial (*antenna*) has to be designed to both collect power from the incoming signal and also to transmit the outbound backscatter signal. The response of a passive RFID tag is not just an ID number (GUID): tag chip can contain nonvolatile EEPROM(Electrically Erasable Programmable Read-Only Memory) for storing data. Lack of an onboard power supply means that the device can be quite small: commercially available products exist that can be embedded under the skin. The smallest such devices commercially available measured 0.4 mm × 0.4 mm, and is thinner than a sheet of paper; such devices are practically invisible. Passive tags have practical read distances ranging from about 2 mm (ISO 14443) up to about few metres(ISO 18000-6) depending on the chosen radio frequency. Due to their simplicity in design they are also suitable for manufacture with a printing process for the antennae. A development target are polycarbon semiconductor tags to become entirely printed. Passive RFID tags do not require batteries, and can be much smaller and have an unlimited life span.

Semi-passive RFID tags are very similar to passive tags except for the addition of a small battery. This battery allows the tag IC to be constantly powered. This removes the need for the aerial to be designed to collect power from the incoming signal. Aerials can therefore be optimised for the backscattering signal. Semi-passive RFID tags are faster in response and therefore stronger in reading ratio compared to passive tags.

Active RFID tags or *beacons*, on the other hand, have their own internal power source which is used to power any ICs and generate the outgoing signal. They may have longer range and larger memories than passive tags, as well as the ability to store additional information sent by the transceiver. To economize power consumption, many beacon concepts operate at fixed intervals. At present, the smallest active tags are about the size of a coin. Many active tags have practical ranges of tens of metres, and a battery life of up to 10 years. Because passive tags are cheaper to manufacture and have no battery, the majority of RFID tags in existence are of the passive variety.These tags cost an average of Euro 0.20 at high volumes. Today, as universal RFID tagging of individual products become commercially viable at very large volumes, the lowest cost tags available on the market are as low as 7.2 cents each in volumes of 10 million units or more. Current demand for RFID integrated circuit chips is expected to grow rapidly based on these prices. There are four main frequency bands for RFID tags commonly in use. They are categorized by their radio frequency: low frequency tags (125 or 134.2 kHz), high frequency tags (13.56 MHz), UHF tags (868 to 956 MHz) or 463 MHz, and microwave tags (2.45 GHz or 5.8 GHz). UHF tags can be used globally when specially tailored according to regional regulations as there are no globally unified regulations for radio frequencies in this ISM band range. There is a wide variation of transponder devices and contactless chip cards which deliver similar functions.

## Who's using RFID?

RFID is already in use all around us. Ever chipped your pet dog or cat with an ID tag? Or used an EZ Pass through a toll booth? Or paid for gas using Exxon Mobil's' SpeedPass? Then you've used RFID.

Some uses, especially those related to security, seem like a great idea. For instance, Delta is testing RFID on some flights, tagging 40,000 customer bags in order to reduce baggage loss and make it easier to route bags if customers change their flight plans.

Three seaport operators - who account for 70% of the world's port operations - agreed to deploy RFID tags to track the 17,000 containers that arrive each day at US ports. Currently, less than 2% are inspected. RFID tags will be used to track the containers and the employees handling them.

The United States Department of Defense is moving into RFID in order to trace military supply shipments. During the first Gulf War, the DOD made mistakes in its supply allocation. To streamline operations, the U.S. military has placed RFID tags on 270,000 cargo containers and tracks those shipments throughout 40 countries.

On a smaller level, but one that will instantly resonate with security pros, Star City Casino in Sydney, Australia placed RFID tags in 80,000 employee uniforms in order to put a stop to theft. The same idea would work well in corporate PCs, networking equipment, and handhelds.

In all of these cases, RFID use seems reasonable. It is non-intrusive, and it seems to balance security and privacy. Other uses for RFID, however, may be troublesome.

Visa is combining smart cards and RFID chips so people can conduct transactions without having to use cash or coins. These smart cards can also be incorporated into cell phones and other devices. Thus, you could pay for parking, buy a newspaper, or grab a soda from a vending machine without opening your wallet. This is wonderfully convenient, but the specter of targeted personal ads popping up as I walk through the mall, a la *Minority Report*, does not thrill me.

Michelin, which manufactures 800,000 tires a day, is going to insert RFID tags into its tires. The tag will store a unique number for each tire, a number that will be associated with the car's VIN (Vehicle Identification Number). Good for Michelin, and car manufacturers, and fighting crime. Potentially bad for you. Who will assure your privacy? Do you really want your car's tires broadcasting your every move?

The European Central Bank may embed RFID chips in the euro note. Ostensibly to combat counterfeiters and money-launderers, it would also enable banks to count large amounts of cash in seconds. Unfortunately, such a move would also makes it possible for governments to track the passage of cash from individual to individual. Cash is the last truly anonymous way to buy and sell. With RFID tags, that anonymity would be gone. In addition, banks would not be the only ones who could in an instant divine how much cash you were carrying; criminals can also obtain power transceivers.

Several major manufacturers and retailers expect RFID tags to aid in managing the supply chain, from manufacturing to shipping to stocking store shelves, including Gillette (which purchased 500 million RFID tags for its razors), Home Depot, The Gap, Proctor & Gamble, Prada, Target, Tesco (a United Kingdom chain), and Wal-Mart. Especially Wal-Mart.

The retail giant, the largest employer in America, is working with Gillette to create "smart shelves" that can alert managers and stockboys to replenish the supply of razors. More significantly, Wal-Mart intends for its top 100 suppliers to fully support RFID for inventory tracking by 2005. Wal-Mart would love to be able to point an RFID reader at any of the 1 billion sealed boxes of widgets it receives every year and instantly know exactly how many widgets it has. No unpacking, no unnecessary handling, no barcode scanners required.

## WHY ONLY RFID ?

Right now, you can buy a hammer, a pair of jeans, or a razor blade with anonymity. With RFID tags, that may be a thing of the past. Some manufacturers are planning to tag just the packaging, but others will also tag their products. There is no law requiring a label indicating that an RFID chip is in a product. Once you buy your RFID-tagged jeans at The Gap with RFID-tagged money, walk out of the store wearing RFID-tagged shoes, and get into your car with its RFID-tagged tires, you could be tracked anywhere you travel. Bar codes are usually scanned at the store, but not after purchase. But RFID transponders are, in many cases, forever part of the product, and designed to respond when they receive a signal. Imagine everything you own is "numbered, identified, catalogued, and tracked."

All are talking about placing RFID tags into all sensitive or important documents: "it will be practical to put them not only in paper money, but in drivers' licenses, passports, stock certificates, manuscripts, university diplomas, medical degrees and licenses, birth certificates, and any other sort of document you can think of where authenticity is paramount." In other words, those documents you're required to have, that you can't live without, will be forever tagged.

Consider the human body as well. Applied Digital Solutions has designed an RFID tag - called the VeriChip - for people. Only 11 mm long, it is designed to go under the skin, where it can be read from four feet away. They sell it as a great way to keep track of children, Alzheimer's patients in danger of wandering, and anyone else with a medical disability, but it gives me the creeps. The possibilities are scary. In May, delegates to the Chinese Communist Party Congress were required to wear an RFID-equipped badge at all times so their movements could be tracked and recorded. Is there any doubt that, in a few years, those badges will be replaced by VeriChip-like devices? Surveillance is getting easier, cheaper, smaller, and ubiquitous. Sure, it's possible to destroy an RFID tag. You can crush it, puncture it, or microwave it (but be careful of fires!). You can't drown it, however, and you can't demagnetize it. And washing RFID-tagged clothes won't remove the chips, since they're specifically designed to withstand years of wearing, washing, and drying. You could remove the chip from your jeans, but you'd have to find it first.

That's why Congress should require that consumers be notified about products with embedded RFID tags. We should know when we're being tagged. We should also be able to disable the chips in our own property. If it's the property of the company we work for, that's a different matter. But if it's ours, we should be able to control whether tracking is enabled.

Security professionals need to realize that RFID tags are dumb devices. They listen, and they respond. Currently, they don't care who sends the signal. Anything your companies' transceiver can detect, the bad guy's transceiver can detect. So don't be lulled into a false sense of security. With RFID about to arrive in full force, don't be lulled at all. Major changes are coming, and not all of them will be positive. The law of unintended consequences is about to encounter surveillance devices smaller than the period at the end of this sentence

## THREATS FOR THE RFID TAGS

The basic functionality of RFID systems is to provide identification of individual objects by the replies the attached RFID tag sends to a request performed by a reader. The reader uses an attached database to link the received ID number to a specific object described in the database. The major drawback of those systems is that the communication scheme does not provide a method to prove the claimed identity. Since a typical tag answers its ID to any reader (without a possibility to check whether a reader is authorized to receive the information), and the replied ID is always the same, an attacker can easily forge the system by reading out the data of a tag and duplicating it to bogus tags. Closed RFID systems with common access of all readers to a central database, can check for illegal duplicates (bogus tags) within the database but this is not

practical for many applications. Furthermore, it is impossible to distinguish the original tag from its illegal duplicates.
Strong authentication mechanisms can solve uprising security problems in RFID systems and therefore give protected tags an added value. The three main security threats in RFID systems are forgery of tags, unwanted tracking of customers, and the unauthorized access to the tag's memory.

## WHY IS AUTHENTICATION TECHNIQUE REQURIED

So here, we propose authentication protocols for RFID systems.These protocols allow protecting high-value goods against adversary attackers. Additionally, we show that these protocols are feasible for nowadays restriction concerning data rates and compliance to existing standards as well as the requirements concerning chip area and power consumption. With authentication we mean a method to provide a proof for a claimed identity. This proof is based on a secret stored within the authenticating part of the system. As long as the secret information stays secret and the used protocol does not leak sensitive information, an attacker cannot forge a tag.
A communication system providing authentication can reject access (to information, entry, etc.) to non authorized parties. To keep the authentication secure, it is necessary that an attacker does not gain information about the secret by listening passively to successful authentications. To fulfill this requirement for strong authentication, it's necessary to use cryptographically strong computation .Under "cryptographically strong" in this context we understand that it must be computationally infeasible with current computing systems to derive the secret key data from an unlimited number of known input and output message pairs.

## SYMMETRIC AUTHENTICATION

Authentication is the mechanism that one entity proves its identity to another entity. Strong authentication protocols, such as challenge-response protocols (standardized in ISO/IEC 9798) are widely used in practice today. In challenge-response protocols, one or several messages are exchanged between the party who wants to prove its identity (the claimant) and the party who wants to verify the identity (the verifier). This is called the protocol. In a typical scenario, the verifier challenges the claimant with an unpredictable value that is used no more than once (the nonce). The claimant is required to return a response that is depending on the nonce and on the stored secret.

Using strong authentication for RFID systems leads to significant security enhancements. If readers are required to authenticate themselves to tags, attacks such as unwanted tracking and unauthorized memory access are rendered infeasible. If tags are required to authenticate themselves against readers forgery of tags is prevented. It is advantageous to use standardized protocols and algorithms because they have been rigorously cryptanalyzed and are widely used. Hence, systems based on standardized protocols and algorithms are more likely to be secure and interoperable with other well established infrastructures. Standardized challenge-response protocols are defined upon symmetric-key and asymmetric-key cryptographic primitives.
Using symmetric-key cryptography has the disadvantage that there is one secret key shared through all parties. If one key is compromised for any reason the whole systems gets insecure. However, strong asymmetric-key cryptography requires extremely costly arithmetic operations and is therefore out of question for RFID systems today. Strong symmetric-key cryptographic primitives include encryption primitives such as AES [5] which allow compact implementations [1]. In the following, a few authentication protocols based on challenge-response methods are explained

### A. Tag Authentication

Here, the tag authenticates itself against a reader. The origin of the tag can be proved and forgery is prevented. The protocol works as follows (we denote the concatenation of values by |):

Reader Tag: AuthRequest | ID | $R_R$

Tag Reader: $E_K(R_R | R_T) | R_T$

The reader sends an authentication request, addressed with the ID of the tag (8 bytes). It contains a nonce, generated by the reader ($R_R$, 8 bytes). The tag encrypts the nonce with the secret key and sends the result back to the reader, which can then verify the result. To avoid chosen-plaintext attacks, i.e. that an attacker can fix the value of $R_R$ and can therefore control the input for the encryption, the tag can itself generates a nonce ($R_T$, 8 bytes) to "hide" the challenge. The use of $R_T$ is optional.


Figure 2 A-SRAC protocol

### B. Reader Authentication.

This method is used for authenticated access to the tag's memory. The tag requests an authentication from the reader before it reveals its true ID and further access to the tag. The tag takes part in the anti-collision algorithm with a random ID ($R_T$, 8 bytes). All addressed requests are done with $R_T$ (tracking prevention). Only after successful authorization of the reader, the tag sends its ID in plaintext and grants the reader access to the memory. Attackers can get the ID by passively listening to the communication, although they are not able to initiate it. Another problem could be hijacking of an authorized connection. It has to be analyzed if this is a realistic security threat for real-world applications.

Reader Tag: ReaderAuth | $R_T$ | $E_K(R_T | R_R) | R_R$

Tag Reader: ID

When answering to the inventory request, the tag indicates with a flag that the reader has to authenticate itself. The reader answers to the challenge ($R_T$, 8 bytes) and sends a request to reveal the tag's ID. To avoid a chosen-plaintext attack, the reader can generate a nonce $R_R$ and combine it with $R_T$ before answering the challenge.

### B. Mutual Authentication.

In mutual authentication, both parties authenticate themselves against each other. All three security threats (unwanted tracking, unauthorized memory access, and forgery) can be prevented. Like in the former protocols the tag answers the inventory request with a nonce ($R_T$, 8 bytes), and requests authentication from the reader. The reader answers the challenge and sends another

challenge ($R_R$, 8 bytes) for the tag. The tag answers the reader's challenge and both are authenticated. The ID is never sent in plain, so unwanted tracking is prevented.

Reader → Tag: MutualAuth | $R_T$ | $E_K(R_T | R_R)$ | $R_R$

Tag → Reader: $E_K(R_R | ID)$

## REQUIREMENTS OF AUTHENTICATION IN CURRENT RFID SYSTEMS

The security-enhanced RFID system is mainly based on the standard ISO 18000 [7]. This standard defines the operating conditions under which these RFID tags are operated. It defines the carrier frequency which is 13.56 MHz and defines the modulation of data. The communication between the reader and the tag uses Amplitude Shift Keying and the response from the tag works via load modulation because the tag has no active power supply. Thereby, a resistance is periodically switched on and off using a defined frequency to submit data. Furthermore, the standard describes the data coding mechanisms and defines the overall communication scheme. The tag is not allowed the send to the reader unless data were requested. The communication is initiated by the reader with a request and the tag responses.

### A. Protocol Extension.

The most important command is the anti-collision sequence which is a command every tag has to implement. Thereby, the reader sends an initial inventory command. All tags in the environment make a response which is the tag's unique ID. If only one tag answers to the request the ID can be retrieved by the reader and all subsequent commands can be addressed using the ID which addresses one single tag. If two or more tags make an answer to a request a collision occurs. This can be detected at the reader. The reader then uses a modified inventory request where it adds a part of the tag's ID to the request. Only tags which have this part of the ID are allowed to answer. Once the ID of one tag is identified, the reader sends a "stay quiet" command to the tag with the identified ID. This method is used as long as there are no more collisions and all tags within the environment are identified.

Adding an authentication command to the ISO 18000 standard works by using a custom command which can be defined. The challenge-response protocol fits ideally to the overall request-response protocol. When authenticating a tag, the reader sends a challenge within the request and the tag answers according to the presented authentication protocol.

### B. Interleaved Authentication Protocol.

The authentication protocol mentioned above only works when the result of the cryptographic primitive is available within the time defined for the tag's response. As this time is very short a modification of this authentication scheme was proposed where the calculation time for the algorithm is of minor importance. For this purpose, authentication is split into two parts. The first part is the authentication request (AR), which tells the tag to encrypt the challenge and does not expect any response. The second part is the response request (RR), which collects the authentication response, when the result is available. For one tag, the timing overhead is large, but with more than one tag, the reader can use the idle time (during the tag is busy calculating) to send authentication requests (or other requests) to other tags. This mechanism is outlined in figure 2.


Figure 2: Interleaved authentication protocol.

Figure 2: Interleaved authentication protocol.

**D. Random Number Generation.**

Some of the protocols presented in section II need some kind of random numbers (nonces). Thereby, it is important that not really true random numbers are necessary. The only important thing is that the numbers are not predictable and they must not be duplicated. The implementation on an RFID tag could be a linear feedback shift register (LSFR) where the seed value is applied from an authenticated reader.

## OBJECTIVES OF THIS AUTHENTICATION TECHNIQUE:

1. Raise existing protocol standards for RFID technology with respect to security features.
2. Design and implement tags with strong cryptographic algorithms and implement a prototype tag and a reader.
3. Improve long-range readers in terms of operating range by using innovative architectures.
4. Investigate potential new application fields.
5. Research the role of secure smart tags as part of a world of ambient intelligence.