

Privacy in Radio Frequency Identity Documents

Tres Wiley, Director of eDocuments
Texas Instruments

Executive Summary

The use of contactless technology in identity documents is new and drawing significant attention by the lay and technical press, legislators and policy makers at the state and national levels, and a variety of pundits and privacy advocates. Examples of these technologies include the new United States passport, which began in August of this year to include a contactless chip to improve the security of the passport; the Western Hemisphere Travel Initiative PASS card, which is expected to include a contactless chip; and the more secure drivers' license, which was mandated by the Real ID Act of 2005 and may well include a contactless chip. The situation is a complex one, with concerns over security and user privacy being voiced by many. These concerns, whether real or imagined, must be addressed if the technology and its benefits are to be adopted by our governments and society at large.

This paper describes privacy concerns being voiced today regarding the use of contactless technologies in identity documents, the differences between RFID and contactless smart card systems, and the methods available in each of these systems to protect privacy. The paper concludes with privacy recommendations for how contactless technologies should be used in ID documents.

Contactless Technology Primer

The term RFID is extremely broad, encompassing a range of technologies that have evolved over more than 20 years to fit a wide variety of applications. All RFID systems, however, consist of a tag and a reader. (See Figure 1) The tag is the mobile element and identifies the item to which it is attached. The tag contains a semiconductor chip (or set of chips) and an antenna that relays radio frequency signals into and out of the chip(s).

These chips can be simple or highly complex depending on the application. The chips can include megabytes of memory or only a simple identifying number. The memory can be alterable (read/write) or it may contain fixed information that can be programmed on the chip only once. The chips can contain a sophisticated processor with cryptographic elements to protect the data or they may simply respond to all requests for the information contained on the chip. Lastly, the chip contains a miniature radio to enable it to communicate with the reader using radio frequency waves.

The reader enables the user to remotely determine the information on the tag and to possibly modify the information on the tag. The reader also contains a radio and is typically connected to a host computer or a display device to enable the binary data on the chip to be translated into a form that is useful to humans.

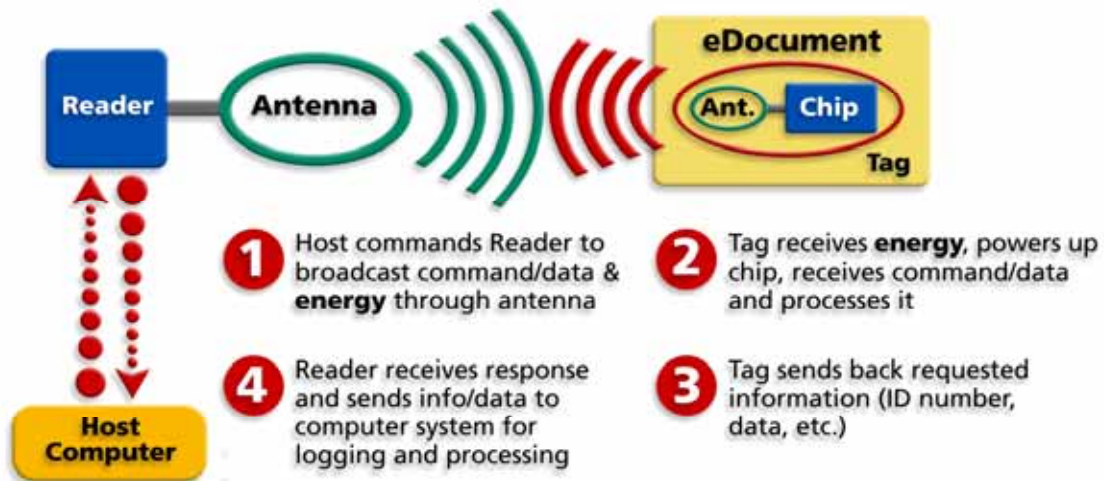


Figure 1: Passive Contactless RFID

The nature of the RF link between the tag and the reader is a critical one which determines much of the level of performance of the RFID system, including the maximum range that can exist between the tag and the reader if they are to communicate, the speed at which data can be moved between the tag and the reader, and the susceptibility of the communication between the tag and the reader to be blocked or attenuated by materials between the tag and the reader.

In the end, however, the RF link is merely a communication pipe that replaces a wire with a bidirectional wireless radio path.

One important characteristic that can be used to eliminate those RFID technologies that are not applicable to identity documents is whether or not the tag contains a standalone power source. In the case of ID documents, the tags do not contain a battery due to their cost, size, and limited life. Such tags without batteries are called passive tags and instead rely on the reader to supply energy to the chip via the reader's RF field which is captured by the tag's antenna. Therefore, in the case of passive tags, the reader has two functions: to energize the chip so it can communicate and to send/receive data to and from the tag. The effective range of passive tags is limited both by the distance at which adequate energy can be transferred to the tag to power-up the chip and the range at which the weak signal transmitted by the tag can be heard by the reader. Ultimately, however, if the chip does not receive enough energy from the reader, it cannot transmit its identity.

Passive tags today communicate with and derive energy from their readers using one of three broadly licensed radio frequencies: 125/134KHz, 13.56MHz, and 900MHz. (There are other frequencies used, but they are much less common and none of them are relevant to ID applications.) The propagation characteristics of RF fields corresponding to these frequencies are markedly different and have been selected to optimize the system performance in specific applications.

The range of the 125/134KHz system is less than two meters but can easily penetrate ionic liquids. It is the oldest RFID technology and is most commonly used today for animal tagging and access control into buildings.

The 13.56MHz systems typically operate according to one or the other of two protocols defined by international standards, ISO 15693 or ISO 14443. These 13.56MHz systems are also able to penetrate ionic liquids like those of the human body. ISO 15693 has a maximum range on the order of two meters but operates at a relatively low data transfer rate. ISO 14443 has a maximum range on the order of four inches but operates at a relatively high data transfer rate. The ISO 14443 technology with its higher data rates is commonly used today in newer access control systems, contactless payment systems like the American Express ExpressPay and MasterCard PayPass™, and the new electronic passport. The ISO 15693 technology is commonly used in longer range access control systems and inventorying library books.

The 900MHz system has a maximum range on the order of 10 meters but suffers from an inability to penetrate ionic liquids in its longer range mode of operation. This technology is commonly used today in tagging cartons and pallets of goods

in the commercial supply chain and vehicular access control, such as busses into controlled areas.

Comparison of RFID and Contactless Smart Cards

Frank Lloyd Wright once said, “Form follows function.” Like many things in the modern world, the design of RF enabled chips is no exception. One reason, of course, is that the electronics market is highly competitive and economically efficient. Companies have readily designed chips that are optimized for each of the wide variety of tagging applications, tailoring the chips’ performances to meet the specific functional requirements of each application and carrying no superfluous functionality.

The critical functional performance parameters which RF chips must meet vary from application to application but almost always include the following:

- Range between the tag and reader
- Amount of data to be contained on the chip
- Number of tags to be identified by the reader at one time
- The rate at which data must be moved on and off the chip
- Whether the data on the chip will be static or dynamic
- Physical characteristics of the item carrying the tag and the environment in which the tag is used
- The magnitude of the threats to compromise in the use of the tag
- The consequence of a successful compromise in the use of the tag

The chips designed for animal tagging are different from those used to tag library books, or those used to track factory totes on assembly lines, or those to track cartons and pallets of goods going through the supply chain. The reason they are all different is that the critical functional performance values for one or more of these eight parameters are distinct for each application.

While all of these applications are the domain of traditional RFID technologies, and while they differ from one another in several of the first six parameters listed above, they all share a common view with respect to the seventh and eighth parameters. The magnitude of the threats and the consequences of having a criminal hacker successfully compromise the chip or the RF communication between the chip and the reader are low. Criminals tend to be rational people, at least those involved in high-tech crimes, and will invest their energies in hacking systems where the returns are high, not those where the returns are low. For example, criminals are not motivated to expend much energy to counterfeit a tag on a carton of toilet paper in order to steal one carton. And, even if they do, the amount of harm done is very low. Customers for such RFID chips, therefore, are

not motivated to pay for chip security mechanisms to protect against an unlikely threat with minor consequences in the event they occur.

A good example of this logic in the market place is the RFID tag mandated by Wal-Mart for use in its supply chain.

- Range between the tag and reader: Up to 30 feet to enable pallets to be read by forklift trucks passing down aisles in distribution centers
- Amount of data to be contained on the chip: Single, unique 96 bit number
- Number of tags to be identified by the reader at one time: Possibly hundreds
- The rate at which data must be moved onto and off the chip: Very fast when cartons are moving at 20 feet per second down a conveyor belt or when a pallet of cartons comes through a warehouse dock door at 15mph.
- Whether the data on the chip will be static or dynamic: Static, since the identification number of a carton of dish towels isn't going to change.
- Physical characteristics of the item and the environment in which the tag is to be attached: Highly variable.

The resulting chip is one now defined by an international standard, ISO 18000-6c. The tag operates at a UHF frequency to enable tag reads at extended ranges, has a very small memory that can be locked by providing a simple password (not changeable), and has a highly tuned scheme to enable a reader to correctly identify hundreds of tags simultaneously. This tag is expected to be low cost because the cost of the chip is critical to the economics of the supply chain application. Extra circuitry elements to prevent unlikely compromises by criminals were consciously eliminated to lower the cost and improve the performance in several other key areas.

In stark contrast to the traditional applications of RFID are the uses of RF enabled chips in payment systems or identity documents where the threats of compromise are high and the consequences of having a criminal successfully compromise a chip or the communication between the chip and the reader are high.

Chips optimized for these two sensitive applications typically have the following characteristics:

- Range between the tag and reader: On the order of 4 inches
- Amount of data to be contained on the chip: Many kilobytes of data
- Number of tags to be identified by the reader at one time: 1, but possibly up to 10
- The rate at which data must be moved onto and off the chip: Extremely fast to keep user transaction times down to an acceptable level.

- Whether the data on the chip will be static or dynamic: Usually dynamic to enable data transmissions to be encrypted with different keys each time the chip is read although some systems/applications are done with static data transfers.
- Physical characteristics of the item and the environment in which the tag is to be attached: Benign but performance must not be compromised by having a human hand (ionic liquid) holding the document
- The magnitude of the threats to compromises in the use of the tag: Large to enormous
- The consequence of a successful compromise in the use of the tag: Large to enormous

Not surprisingly, the chip(s) tailored to these functional requirements are materially different than those for animal tagging or supply chain applications. Here, too, international standards, ISO 14443 and ISO 7816, have been defined to enable multiple companies to produce highly secure tags and readers that are interoperable.

Privacy Concerns & Contactless Technologies

Current literature describing the variety of privacy concerns people have with RF enabled identity documents shows a range of concerns that can appear quite large, not because the fundamental issues are so numerous, but because the language to describe them is so varied that they appear different. In fact, many are identical but just called by different names by different authors or are slight variations on scenarios of risk that are actually reflecting the same basic issue. This section will categorize these privacy concerns and distill them into a simple set of distinct issues to be addressed technically or by policy.

Throughout this section of the paper I will be describing the perpetrator of the subject misbehavior as a criminal. In most scenarios such behavior by a perpetrator would indeed be unlawful, in others the behavior would at least be considered unethical or immoral. I am not using the term “hacker,” because it is a term that can describe someone attempting to break a system for ethical or unethical purposes. This usage could be confusing in this regard. The harm to an ID system or ID holder is done by a perpetrator intent on misusing a system for their own gain. Regardless of their legal status, I will refer to them as criminals.

Electronic identity documents of any sort, either traditional contact smart cards or RF enabled contactless cards, are subject to three fundamental threats:

- The owner's personally identifiable information is somehow taken or stolen without the owner's knowledge, allowing the criminal to impersonate the owner and ruin their reputation or incur unwanted liabilities that will be borne by the true owner.
- The owner's anonymity is potentially compromised when their actions or movements are recorded by others, including the government, as they go through their daily activities, doing things that would not normally require the owner to divulge their identity.
- The threat to an individual, or to society in general, when a criminal creates a counterfeit identity document that enables the criminal to operate in society with the privileges of a rightful owner of a legitimate identity document.

So, what is the difference between an RFID tag and a contactless smart card? It's the level of security designed into the chip to counter the expected possible threats of criminals. The fact of the matter is that highly secure chips could be built at any of the common contactless frequencies (125/134KHz, 13.56MHz, and 900MHz) if all of the expected threats were adequately countered by one or more elements of the chip/reader/system design. To date, however, because the operational requirements for electronic ID documents have only required operation at short ranges, on the order of a few inches, and because the transaction time must be short, the 13.56MHz frequency with high data transfer rates (ISO 14443) has been chosen by users and technology providers. When considering specific threats to privacy and security, the ad hoc use of traditional RFID chips designed for identification and tracking of things stands in stark contrast to contactless smart cards designed with strong security features for identity document applications.

Below, each of the specific threats to privacy associated with contactless technologies is described in detail along with a comparison between RFID and contactless smart card implementations of an electronic ID system.

Loss of Personal Information

Loss of personally identifiable information, such as date of birth, address, phone number, social security number or mother's maiden name, is a topic of concern as identify theft is reportedly one of the fastest growing crimes in the United States. In the context of RF enabled ID documents, the fear is that a sophisticated criminal could take the information off the cards without the knowledge of the owner. Two scenarios are often described, one of skimming in which the criminal has a rogue reader and is able to directly take the information from the document that's still in the possession of the owner, and eavesdropping in which the criminal listens at a distance to an electronic transaction between an ID document and a legitimate reader and overhears the identity information as it

is being conveyed from the document to the reader. In both scenarios the concern is that by using an RF link between the ID document (tag) and the reader the risk of losing the personally identifiable information is too high.

Skimming: Chips that allow any reader to gain access to the information on the chip are clearly at risk. The strongest protection employed on RFID chips to limit access is a simple password, typically no more than 32 bits. This compares with 128 bits keys used today to limit access to secure smart card chips. The range over which a chip can be activated also figures into the vulnerability of the chip with respect to skimming. Chips that can be read at a distance beyond a few centimeters are clearly more vulnerable to an attack by criminals than chips that can only be read at a range of four inches. Combining the relatively weak security of RFID chips with their longer read ranges makes them much more vulnerable to attack than contactless smart card chips.

Eavesdropping: If an attacker can overhear the data transfer, the question arises as to whether the information is encrypted in a secure manner or merely transferred “in the clear” (unencrypted). Almost all RFID chips transfer the data “in the clear” but there are a few that can encrypt the data, notable among these few is the EPC Gen 2 chip defined by ISO 18000-6c. However, the key length used to encrypt its data is only 32 bits. In comparison, contactless smart cards today typically use key lengths of 128 bits in mathematically robust algorithms to encrypt the data being sent through the air via the RF link. The range over which the data transfer can be heard places most RFID implementations at a comparative disadvantage with respect to contactless smart cards since a criminal will have a harder time eavesdropping on an RF signal in a system designed to operate at four inches than one designed to operate at 30 feet, for example.

Loss of Anonymity

This form of privacy threat envisioned by the use of RF enabled ID documents is quite simple and is based on the ability to read RF tags from a distance. The simplest scenario, tracking, is the one in which the movements of an individual are monitored and subsequently recorded by placing readers at a series of fixed locations and surreptitiously identifying the individuals passing by the readers. Another scenario is one of hot-listing in which a reader is pre-programmed to watch for a specific individual or member of a groups of individuals carrying RF-enabled ID documents and then to cause some action to be taken. The most sinister version of this scenario is the triggering of a terrorist attack after a specific individual has been electronically identified.

The tracking scenario is accomplished by activating a chip, determining its identity through the interrogation of unique information contained on the chip, and

electronically following the individual at some distance. Clearly tracking a chip with a read range of 30 feet is dramatically more feasible than tracking one with a range of less than a foot or two. It is reasonable to state that it is impractical to unobtrusively track a person carrying a contactless smart card with a chip read range of four inches. In fact, it's probably impractical to track someone carrying an ISO 18000-6c tag, but the argument can be made that with enough effort a criminal might be able to do it if they were determined and electronically astute. One has to wonder, though, why they wouldn't employ traditional gumshoe techniques to "tail" the person rather than carry a relatively large antenna, reader, and battery to follow someone from a distance of 30 feet or less. (One misconception is that RF enabled ID documents can be tracked by satellite. This is not the case, unless the satellites are orbiting at an altitude of less than 30 feet.)

A more subtle form of tracking is described by some who are concerned with the use of chips in electronic documents, but it relies on collecting the reads of a contactless ID document in a database as it is used legitimately by an ID holder in a sequence of locations. For example, a passport with a chip that is read at the airline ticket counter leaving the U.S., then at immigration entering a foreign country, and then at U.S. immigration upon return does constitute a form of tracking that is enabled by the contactless technology. Such a definition of tracking does not actually rely on the RF chip, though, to accomplish the tracking. Such tracking can and is done today with traditional, non-IC passports. In this expanded definition of tracking, the use of the RF link does not suddenly make the tracking feasible and is not a legitimate concern distinctly attributable to the use of contactless chips in ID documents.

Hot-listing occurs when a criminal places a reader in a fixed location and programs it to alarm when a specific chip comes into range, thereby inferring the presence of the legitimate ID or document holder. For this attack to work, the reader has to activate the chip and get information from it associated with a specific individual. As is true in tracking, the greater the range capability of the chip/reader system, the easier this scenario is to affect. RFID chips that are optimized for supply chain applications requiring 30 foot read ranges will be more vulnerable than an ISO 14443 chip that can be read at four inches. Assuming the chips have been successfully activated by the reader, at either four inches or 30 feet depending on the technology, the next question is whether the reader can derive information from the chip that would allow the reader to identify chip as the one it was programmed to find. In both RFID and contactless smart card technologies, some chips use a random identifier (as opposed to fixed identifier) to initiate the communication between the chip and the reader, making it impossible to simply identify a specific chip without providing a password to make the chip yield its absolute identity. In these cases where the initial random identifier is used, the strength of the protection given to the absolute identity will

be different between RFID chips and contactless smart card chips. As discussed earlier, the strong, 128 bit key cryptographic protection provided by a contactless smart card chip will make determining its identity extremely difficult in comparison to an RFID chip protected with an 8, 16, or 32 bit key.

Electronic Impersonation

Counterfeiting is the fraud perpetrated by making a new chip in a fraudulent ID document act as if it were one produced by a legitimate issuing authority. RFID chips are not protected against this sort of fraud because of the cost of adding features in the chip to prevent it. The contactless smart card chip achieves its security from this sort of attack by protecting a secret piece(s) of information on the chip that is only known to the legitimate issuing authority. This protection can include extra metal layers, circuits that will erase the secret in the event the chip is probed, circuits that scramble the secret as it is transported around the chip to frustrate sophisticated attempts to listen to electromagnetic signals radiating from the chip, and other highly sophisticated, but costly countermeasures. If the counterfeiter cannot identify the secret from a legitimate chip, it is impossible to make a counterfeit that will operate correctly.

Tampering is fraud perpetuated by altering the data on a legitimate chip. The same features that protect secrets on contactless smart cards against counterfeiting also prevent the alteration of data and provide the highest level of protection available today. RFID chips, on the other hand, may or may not be vulnerable to tampering, depending on the type of memory used to store the sensitive data.

Spoofing is fraud perpetuated by building an electronic device that would enable a criminal to impersonate a legitimate electronic credential. This impersonation of a legitimate chip would include the RF communication characteristics, the communication protocol, and the cryptographic secrets used to authenticate the credential. While this attack is easier to accomplish than a counterfeiting attack because the rogue system does not need to be reduced to a chip, the mechanisms that ultimately protect the system are the secrets used to authenticate the chip. Except for these cryptographic secrets, building a rogue electronic device to impersonate a legitimate chip, be it RFID or a contactless smart card, is relatively easy for both classes of devices. Learning the cryptographic secrets is the difficult part of this attack and RFID chips are much more vulnerable because of the relative ease of illicitly learning the secrets from a legitimate RFID chip than from a contactless smart card chip.

A more sophisticated form of spoofing is a relay attack (See Figure 2) in which a rogue reader is placed surreptitiously near a legitimate owner's ID card, a piece of spoofing equipment is placed near a legitimate reader, and the rogue reader

and the spoofing equipment are connected via a high speed link. The idea of this attack is that legitimate data communications occur between the legitimate ID card and a legitimate reader even though the two elements are separated by some distance, and their operation is unknown to the legitimate card holder. In the instance of an access control card, the criminal would be able to gain access to a building. The maximum distance at which this attack has been demonstrated is about 50 meters, but longer distances could likely be achieved. The appropriate countermeasure to this form of attack involves a view of the larger system and requiring the owner of the ID card to provide a second form of authentication to the reader, such as a PIN, password, or a biometric. Once this is done, the legitimate reader cannot be spoofed since the criminal will be unable to present the second form of authentication.

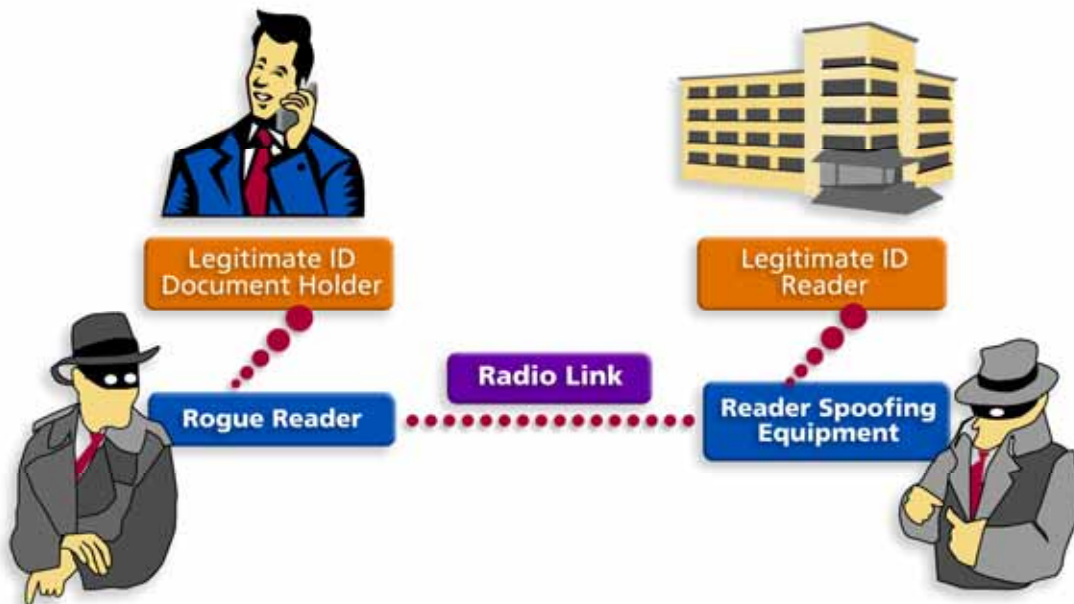


Figure 2: Relay Attack in the Context of Building Access

Conclusions

The imagined and real threats to privacy by the use of RF technologies in electronic ID applications are varied. To the lay person it is easy to confuse the

capabilities of satellite navigation with hand-held terminals (GPS) with the concept of contactless smart cards and assume what can be done with one, can be done with the other. Confusion like this leads to the imagined threat that anyone carrying an RFID tag or contactless smart card can be readily tracked. Such imagined threats can be addressed by the rational explanation of the laws of physics and the facts regarding the design of contactless ID chips, and should not persist in the minds of thoughtful critics.

Real threats to privacy can be dealt with by the appropriate design of the chip, readers, and system level security features as well as the employment of appropriate security policies and system level operating procedures. The use of traditional RFID in ID applications, however, may be potentially dangerous because RFID chips, readers, and systems were not originally designed to protect against the types and levels of threats that are levied against electronic ID documents. While some ID applications may have threat profiles that can be adequately addressed with RFID technology, in general they will not. Should these attacks to RFID-based ID documents be realized, the threats to privacy can be considerable. Conversely, the protections that have been built into contactless smart cards have been optimized to thwart these sophisticated attacks and can be relied upon to protect the privacy of the legitimate ID holder and society as a whole.

About the Author

As director of TI's eDocuments business, Tres focuses on the use of secure RF technology to meet governmental needs for contactless authentication of citizens and travelers. With over six years of experience in the RFID business, he has three years on the tag side of the system as strategy manager for TI's smart label business and nearly three years on the reader side of the system as president of SAMSys Technologies.

Prior to joining TI, Tres worked 20 years in Motorola's government electronics business as engineer, engineering manager, program manager, and business development manager in a range of technologies, including radars, displays, GPS telematics, and cryptography.

About Texas Instruments RFid Systems

Texas Instruments is an industry leader in radio frequency identification (RFID) technology and the world's largest integrated manufacturer of RFID tags, smart labels and reader systems. With more than 500 million tags manufactured, Texas Instruments RFid Systems' technology is used in a broad range of applications worldwide including automotive, document tracking, livestock, product authentication, retail, sports timing, supply chain, ticketing and wireless payment. TI is headquartered in Dallas, Texas and has manufacturing, design or sales operations in more than 25 countries. Texas Instruments is traded on the New York Stock Exchange under the symbol TXN. For more information, contact TI-RFid Systems at 1-888-937-6536 (North America) or +1 972-575-4364 (International), or visit the Web site at www.ti-rfid.com, or the main company site at www.ti.com.

Note: If you make physical copies of this document, or if you quote or reference this document, you must appropriately attribute the contents and authorship to Texas Instruments Incorporated. While every precaution has been taken in the preparation of this document, Texas Instruments Incorporated assumes no liability for errors, omissions, or damages resulting from the use of the information herein. Products or corporate names may be trademarks or registered trademarks of other companies and are used only for the explanation, without the intent to infringe.

©2006 Texas Instruments Incorporated
ALL RIGHTS RESERVED

Important Notice: The products and services of Texas Instruments Incorporated and its subsidiaries described herein are sold subject to TI's standard terms and conditions of sale. Customers are advised to obtain the most current and complete information about TI products and services before placing orders. TI assumes no liability for applications assistance, customer's applications or product designs, software performance, or infringement of patents. The publication of information regarding any other company's products or services does not constitute TI's approval, warranty or endorsement thereof.