Blackboard transact™

Your campus. Connected.

Contactless technology for campus ID systems

Increasing security, convenience, and return on investment for college and university card programs.

Blackboard

Blackboard transact™

Why **Contactless** for campus?

Higher education campus card systems have long relied solely on the magnetic stripe for electronic identification, but this is changing with the emergence of secure, standards-based contactless smart card technology.

Protected between layers of plastic in a contactless card is a built-in computer chip and antenna that enable the card to simply be waved over a reader at the point of acceptance. Contactless cards do not have to be swiped, inserted, or even touched to a reader to conduct a secure transaction. The only requirement is that the card and reader be brought within close proximity of each other – usually one to three inches. Contactless technology is uniquely suited for transactions such as building entry and payment that require speed as well as strong security.

In addition to the ease of use, contactless cards stand apart from other common identification card technologies because of the embedded chip. While barcodes, magnetic stripes, and 125 kHz proximity (prox) cards are simple storage containers for a small amount of data such as an identification number, a contactless card is much more.

Its microcontroller chip can store volumes of information and can add, delete, and perform complex calculations on stored data. It can also carry out on-card functions to ensure system integrity and to manage its interactions with card readers.

The worldwide adoption of contactless technology is diverse, prolific, and expanding exponentially.

- Each of the major credit and debit card brands – Visa, MasterCard, American Express, and Discover – are issuing contactless products.
- Major cities in the U.S. and around the globe rely on the technology to speed riders through ticketing and fare collection in mass transit systems.
- Governments are using contactless technology to secure passports and other identification documents.
- Corporations and educational institutions are using it to secure access to facilities, networks, and privileges.

Contactless benefits

Contactless technology offers significant benefits for applications involving both payment and secure access. The prominence of such applications in a campus environment makes the technology a clear choice for improving the student experience. A series of important, tangible benefits are driving the migration to contactless on college and university campuses:

Higher Security: Contactless technology is uniquely capable of providing optimal transmission security via encryption and a host of other data protection processes.

Reduced maintenance: The nature of the contactless interface reduces the wear and tear on both cards and readers resulting in lower maintenance costs.

Larger memory: Contactless cards can store data equivalent to 100 times that of proximity cards and other ID technologies.

Increased convenience: Consumers enjoy the transaction speed of contactless technology and they also appreciate maintaining possession of their card during a transaction.

Versatile form factors: Contactless technology can be issued in standard ID card form or in a variety of other devices including keychain fobs, watches, stickers, and cell phones.

Future protection: Contactless technology is already replacing magnetic stripe and proximity technology around the globe. Choosing contactless products now can guard against system obsolescence and provide the best avenue for expansion opportunities and overall return on investment.

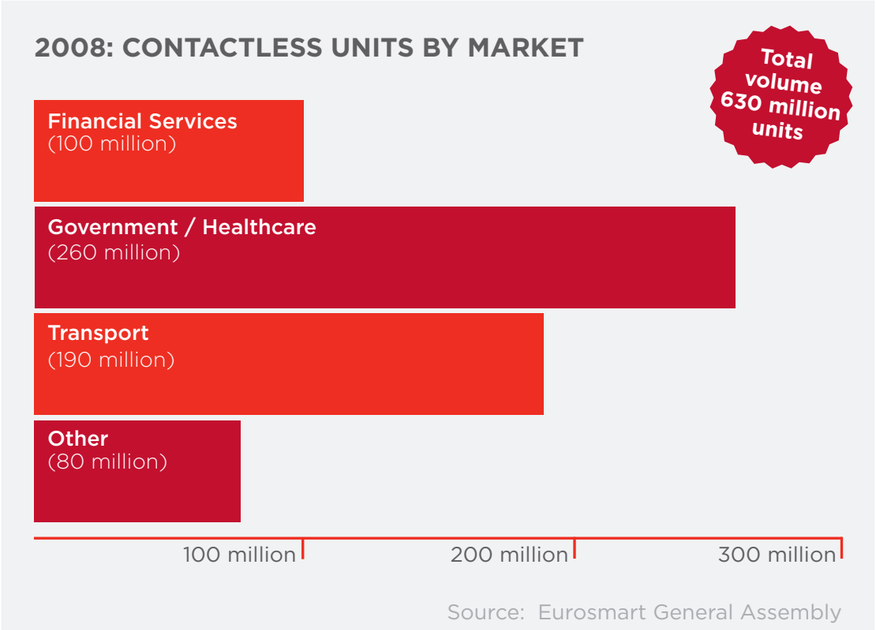
Multiple applications: Carrying a contactless card is like carrying many cards in one. A single contactless card can contain and protect numerous unique ID numbers for different authentication needs. It can also manage multiple applications such as access control, payment systems, cashless vending, and mass transit.

The **Contactless** revolution

Though it may be new to some in the campus market, contactless technology is a well-established, time-tested technology. The number of contactless cards shipped to date is not measured in millions of units but rather billions of units.

Contactless is the fastest growing segment of the identification technology market. According to smart card industry association Eurosmart, 630 million secure contactless cards were shipped in 2008 alone.

Its convenience and security have made it the leading choice for diverse applications and markets including payments, transit, security, and identity.



© 2009 Blackboard Inc.

Payments

Though the volume of contactless payment cards in circulation varies depending on the research or report you read, the numbers are impressive regardless of the source.

- Eurosmart reports that 100 million contactless payment chips were delivered worldwide in 2008 with the U.S. accounting for 75 million.
- First Annapolis forecasts that 100 million contactless payment cards will be in use by 2011.
- Javelin Research estimates that nearly 25 million consumers worldwide will use chip-embedded credit cards for contactless payments this year, and that number is expected to double within five years.
- MasterCard reports that more than 60 million of its contactless cards and tokens had been issued worldwide as of June 2009.

Each of the major payment card associations and brands are offering a contactless card for credit and debit products.

- MasterCard PayPass
- Visa payWave
- American Express ExpressPay
- Discover Zip

A selection of the card issuers offering contactless cards includes Bank of America, Citibank, Citizens Bank, GE Consumer Finance, HSBC, JPMorgan Chase, US Bank and Wells Fargo.

Already more than 150,000 merchants worldwide accept contactless payments. A list of merchant locations includes McDonald's, 7-Eleven, Best Buy, Circuit City, CVS, AMC Theaters, Regal Theaters, Arby's, Wawa, Duane Reade and Sheetz.

Transit

Many of the world's metropolitan areas use contactless cards and tokens to manage ticketing and fare collection for mass transit systems. It is not uncommon for the volume to reach 5, 10 or even 20 million regular users.

In some of the more established programs, the use of these cards has expanded beyond transit to include retail payment as well. Examples of this include London's Oyster card, Hong Kong's Octopus card, and Tokyo's Suica card.

Though the U.S. began issuing contactless fare cards later than other parts of the world, the number of cities has grown rapidly in recent years. Today contactless cards help expedite travel in Atlanta, Boston, Chicago, Houston, Las Vegas, Los Angeles, Minneapolis-St. Paul, New York City, Newark, Philadelphia, San Diego, San Francisco, Seattle, Washington D.C. and more.

Identity

The adoption of contactless travel documents has spread across the globe with more than 100 countries now issuing passports with contactless technology. Identity document research firm Keesing Reference Systems, estimates that more than 100 million contactless passports are now being produced annually.

The U.S. federal government is in the process of issuing a standardized identification card to all employees and contractors. The federal government standard, FIPS 201, defines that every card must have both contact and contactless capabilities. When fully deployed as many as 40 million FIPS 201 compliant cards will be issued.

Around the globe, governments are looking to contactless products to secure travel documents, national ID cards, voter registration cards, and driver's licenses.

Security

Throughout Europe and Asia, contactless cards have been the leading choice for security and access control applications for more than a decade. In the U.S. the widespread use of 125 kHz proximity cards kept the more flexible and secure contactless alternative at bay. In recent years, however, the trend has shifted as more and more corporations, hospitals, and education institutions began the switch from proximity to contactless.

How **Contactless** works

A contactless card is an identification card that contains a computer chip with a connected antenna. This enables it to communicate with a reader over a wireless interface. The chip is also commonly called a semiconductor or integrated circuit (IC) and is functionally the same as those found in personal computers and a myriad of other modern devices.

The term contactless comes from the fact that the card and reader do not need to physically touch during operation. Data is shared between the two through the air in a process known as radio frequency (RF) communication. Just as your car radio receives the data it needs to play music through the air, a contactless card and reader share the data they need to conduct secure transactions through the air.

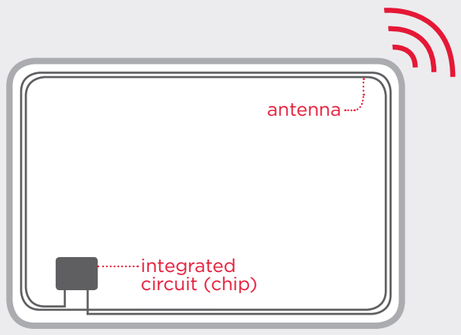
Sharing data via radio frequency communication is extremely common. In addition to AM and FM radio signals, RF communication makes possible many of the conveniences we count on every day including broadcast and satellite television, cordless phones, mobile phones, keyless entry for automobiles, garage door openers, CB radios, wireless networking and more.

In most of these examples of RF communication, both the sender and receiver rely on their own power supply. Contactless cards, however, do not typically contain an on-board power source. Instead, the card accesses the power it needs to operate from the electromagnetic field created by the reader. This process is key to the operation of a contactless identification system as it enables cards to remain idle until they come in close proximity to a compatible reader.

Radio frequency communication is so pervasive that most people simply take it for granted. Yet all around us, vast amounts of data are traveling through the air.

More accurately, electromagnetic radiation (EMR) is traveling through the air and some of it is carrying data. EMR moves in very specific wave-like patterns and while the waves from any one source are of a constant size, different sources of EMR create waves of differing lengths and heights.

It is these variations in wavelength that give rise to the concept of frequency.



A Contactless card contains an embedded computer chip or integrated circuit that is connected to an antenna. When brought within close range of a contactless reader, the card's antenna pulls power from the reader's RF field to turn on the chip and initiate communication.

© 2009 Blackboard Inc.

Frequency

Frequency is the number of waves that occur during a specific time period. It makes sense that longer waves take longer to cycle so there are fewer in a specific time period. Thus the longer the waves the lower the frequency. In more scientific terms, wavelength is inversely proportional to frequency.

The common unit of measure in radio frequency is the hertz. One hertz (Hz) equals one wave per second, one kilohertz (kHz) equals one thousand waves per second, and one megahertz (MHz) is one million waves per second.

Different frequencies of electromagnetic radiation are received or perceived by different receptors. Certain frequencies form visible light when received by the human eye. Others form sound when received by the human ear. The vast majority, however, are imperceptible to humans but can be 'tuned in' by precise mechanical receptors such as radios, mobile phones or contactless card readers.

But just because a device can be set to receive a specific frequency and ignore the noise from others does not mean there is anything meaningful for it to receive. Normal radio waves are little more than an ongoing repetition of the same exact pattern. To use radio waves for the transmission of information, a method to encode data into this constant pattern is required.

The solution is found in a process called modulation. By purposefully and specifically altering the wave pattern its repetition can be interrupted. Through modulation data can be encoded on radio waves by one source, travel across an air interface, and be decoded by another source.

The data is represented in binary form by modulating the waves. Binary data is the process used by computers and other systems to express data using only two conditions or symbols. Computers use zeros and ones, magnetic stripes use positive and negative charges, barcodes use black and white areas, and RF systems use altered and non-altered radio waves.

Each binary digit (e.g. one or zero, modulated or un-modulated wave) is called a bit. Multiple bits together form a piece of data, for example an alphanumeric character. In this manner, RF communication for contactless card systems relies on modulation to encode a stream of bits on a carrier wave to indicate characters. These characters form ID numbers, words, secret keys, and commands or instructions to initiate applications and authorize services.

EXAMPLES OF RADIO FREQUENCY SPECTRUM ALLOCATION

Low frequency	30-300 kHz	AM radio, navigational beacons, proximity cards
High frequency	3-30 MHz	Shortwave radio, citizens band radio, contactless smart cards
Very high frequency	30-300 MHz	FM radio, aviation communications, MRI systems
Ultra high frequency	300-3000 MHz	Broadcast television, mobile telephones, cordless telephones, microwave ovens, RFID tags
Super high frequency	3-30 GHz	Wireless networking, satellite television, garage door openers

More **secure** than other technologies used in campus cards

Contactless technology provides a tremendous increase in security compared to other common ID technologies such as magnetic stripes, barcodes, and conventional 125 kHz proximity (prox) cards. The security increases can be categorized as prevention of unauthorized card creation and the prevention of unauthorized card reading.

Unauthorized card creation

A fake ID that can be used to obtain services, gain access, or make payments creates a fundamental breach in system security. Thus a primary security goal for an identification system is to protect against the fraudulent creation of valid credentials, also known as document fraud.

Three types of fake IDs must be guarded against to ensure a strong level of system integrity:

- Counterfeits – Documents produced by a fraudulent issuer using similar, but non-authentic supplies.
- Genuifeits – Documents produced by a fraudulent issuer using genuine (often stolen) supplies, or produced for unauthorized use on the actual issuer's equipment using genuine supplies.
- Modifeits – Documents that began as legitimate credentials but were altered in some manner for fraudulent use.

A secure system must guard against all three varieties of fraudulent ID cards: **Counterfeits**, **Genuifeits**, and **Modifeits**.

Obviously, the choice of identification technology used has little impact on the visual aspects of the ID. The background images, printed data, and photos look the same whether the card contains a contactless chip, magnetic stripe, or proximity insert. Regardless of the technology, steps can and should be taken to make it difficult for criminals to create visually convincing fake IDs or modify existing IDs. A variety of techniques including micro-printing and holography can help protect the printing and personalization of the visual data.

The choice of identification technology can play a tremendous role, however, in safeguarding against document fraud at the electronic level.

© 2009 Blackboard Inc.

Security through availability

At the first level is security through availability. Though it is not an ideal means, the relative availability of card stock and equipment required for the creation of fraudulent documents impacts security.

Blank magnetic stripe card stock and a card printer with a magnetic stripe encoder are available readily and inexpensively. The blank card stock and encoding hardware for proximity and contactless systems are less readily obtainable and thus a degree of security is afforded these systems simply due to the lower availability.

Security through obscurity

The next level can be thought of as security through obscurity. By not disclosing key elements of a system, a level of security can be obtained. Though cryptographers consider this approach to be wrought with vulnerabilities, it is the fundamental security component of many systems.

The use of obscurity has been all but lost in magnetic stripe systems. Though some vendors encode data on the magnetic stripe in a custom format, the approach does little to provide security because of the ease with which data can be read and analyzed. Obscurity is really only a card swipe away.

For proximity card systems, however, obscurity is a common security approach. The most common proximity card format, known as 26-bit Weigand, is an open format with encoding details made available publicly. But many security system providers and resellers choose to encode their customers' proximity cards in a proprietary data format. This format is kept secret in an attempt to complicate document fraud. Security experts consider this to be a weak attempt at best.

Most modern contactless systems are built upon international industry standards so at the root level there exists little to no obscurity. Data structures within the cards are publicly available in some cases and kept secret in other cases. In reality, however, the third level of security renders both of these prior approaches insignificant when applied to contactless systems.

Security through cryptography

Neither security through availability nor security through obscurity is sufficient for modern identity, access, or payment systems. Security through cryptography is the only real way to prevent document fraud. In fact, an identification technology that does not invoke strong cryptographic-based authentication at the issuance level is susceptible to all three types document fraud: counterfeiting, genuifeiting, and modifeiting.

To create a functional card within a secure contactless system, a series of complex cryptographic protections must be achieved. Chief among these is the authentication of the card issuance hardware via a security access module (SAM) prior to card setup or personalization. The concept of SAM-enabled authentication is described in detail later in the Mutual Authentication section.

Unauthorized card reading

Most of the previous generation of identification technologies – barcodes, magnetic stripes, proximity cards – are designed to store a number and in some cases a small amount of additional data. These technologies were not designed to protect the data encoded. To the contrary, they were designed to make it easy to access stored data to expedite transactions. Most magnetic stripes, barcodes, and proximity cards can be read by any off the shelf reader. Secured data on a contactless card, however, can only be read by an approved reader.

Contactless technology offers both advanced storage capacity and, more importantly, a host of security techniques designed to guard against unauthorized access to the stored data. Among these techniques encryption, mutual authentication, and message authentication coding are essential.

To protect against unauthorized card reading, secure contacless systems use techniques such as **encryption**, **mutual authentication**, and **message authentication coding**.

Encryption

All communications between a card and reader are encrypted. This renders attacks based on eavesdropping on or intercepting of the communication channel ineffective. Even if successfully obtained, any accessed data would be illegible without the symmetric Data Encryption Standard (DES) or triple DES keys used to encrypt the stream.

Message authentication coding (MAC)

A message authentication code (MAC) is a cryptographic technique that is used to ensure that a message is not altered or tampered with during transmission. In essence it is an algorithm that uses the content of the original message and a secret key to create a hash value (also called a message digest).

This digest is transmitted along with the original message. Upon receipt of the message, the recipient uses the same secret key to create its own digest from the content it received. This new version is compared to the one created prior to transmission. If the digests are identical, the message is verified. If not, the message has been altered in some way during transmission.

By verifying MACs for each crucial communication or transaction, the system can be confident that questionable transactions are not entering the system either by fraud, malfunction, or other cause.

© 2009 Blackboard Inc.

Mutual authentication

Two parties – a transponder (card) and a reader – are involved in every contactless transaction. From a security perspective it is crucial that cards only share data with authorized readers and that readers only process transactions from valid cards. This is assured through a cryptographic process known as mutual authentication in which the card and reader independently verify the authenticity of other before initiating a transaction.

The section below provides an overview of the mutual authentication process. The goal is to make this technical subject understandable to all parties. The key benefit of mutual authentication is that it enables cards and readers to establish trust before sharing personal or secure information. Contactless and other smart cards are the only ID technologies that possess this level of sophistication.

When a card enters a reader's RF field and powers on, they cautiously get to know each other. The goal is for each to independently decide if they trust the other party. In essence, each asks the other a question that only a trusted party would know. If the answer is correct, communication continues but if it is incorrect no further data is shared.

At the time of manufacture, every contactless chip receives a unique serial number that is openly available to all standard card readers. This number is not secured in any way and should only be used for low security transactions or those that are secured at the system level using other techniques. This serial number is an important tool, however, in the creation of a derived key for mutual authentication.

A secure contactless system has a master key that is highly secured and protected deep within the central system. This key is protected by a sophisticated series of hardware and software techniques. It exists to create Security Access Modules (SAMs), special chips that are used to distribute the system's cryptographic keys to the individual card readers deployed in the field. If a card reader is stolen the keys are locked within the SAM. If any attempt is made to extract the keys from the SAM, it is designed to sense the activity and destroy the keys.

When a card is initially personalized with applications and data, a secret key is calculated using the system's master key and the card's unique serial number. The secret key is stored in the card. Now the card contains two numbers, the freely available serial number and a protected secret key.

During mutual authentication, the reader requests the card's freely available serial number. In the reader's SAM, the serial number and the system master key are used to recreate the card's secret key. Now both the card and reader possess that individual card's secret key. It is crucial to overall system security that this secret key is valid only for the individual card involved in the transaction. In this way, even if the card or more accurately its key is ever compromised, the system keys are still secure. Additionally, because the SAM is used for recreation of the card's key within the reader the system's master key has never been at risk outside of protected hardware.

Next the card creates a random number and sends it to the reader. The reader creates its own random number and encrypts both numbers using what it calculated to be the card's secret key. It sends this data string to the card.

The card decrypts this string using its secret key revealing the two random numbers. If the first matches the number it created as its random number, the card can be confident that the reader did indeed possess the system's master key. That is because the identical secret key must both encrypt and decrypt the data for the data to match. Because it matches the card knows that this is a trusted reader.

Now it is the card's turn to prove its trustworthiness to the reader. The card takes the second random number, the one selected by the reader, from the decrypted string. It encrypts this number using its secret key and sends the result back to the reader. The reader decrypts this string using what it calculated to be the card's secret key. The decrypted data is examined to see if includes the reader's original random number.

If it does, the card can be trusted. That is because the random number was only provided to the card in encrypted form so for it to match, the card would have to decrypt then re-encrypt the number using its secret key. That secret key would have to match the one that was calculated by the reader.

With both the card and reader confident that of the other's trustworthiness, the sharing of confidential data and the initiation of transactions and services can begin.

In summary, two important things have occurred via this process of mutual authentication. First, bilateral trust is verified prior to any sharing of secure data by the card or reader. Second, by using a secret key that is unique to each card the impact of any possible card breach is limited to that one card only and will not compromise the integrity of the system as a whole.

Why Blackboard Contactless?

Worldwide more than 400 million FeliCa cards, tokens, and mobile chips have shipped and the technology has been securing payments, access, and identity transactions for nearly fifteen years. It has a number of distinct performance, security, and marketplace advantages over the other standardized contactless offerings in the market today.

Performance advantages

From a performance standpoint, FeliCa is the fastest contactless product on the market communicating at speeds of 212 kilobits per second (kbps). This is twice the speed of other contactless products that reach data communication rates of only 106 kbps.

Data transfer speed is essential in contactless transactions to ensure that adequate security procedures can be implemented without sacrificing customer convenience. With FeliCa entire transactions – including card detection, mutual authentication, read and write functions – can be conducted in just one-tenth of a second.

This level of performance is imperative in places like Tokyo, Japan where each day 20 million transactions are conducted using FeliCa cards in the city's mass transit system. Even a fraction of a second delay could mean a virtual shutdown of the city's transit infrastructure.

Security advantages

FeliCa combines speed with security. The chip and operating system were designed to run multiple applications or services on a single card or token. Different services can be protected with unique secret keys to ensure that only appropriate and necessary data is revealed during a transaction.

The mutual authentication process conducted between the card and reader enables each to securely and independently authenticate the other prior to any transaction. With FeliCa's implementation of mutual authentication speed is increased by authenticating to all protected services during a single process. Thus if multiple services are to be accessed in a given transaction, there is no need to conduct separate mutual authentication sessions as each service is initiated.

Data and services are stored on different chips in different ways. FeliCa features an extremely flexible file structure and created a security approach that allows control over access levels to various services and even to functions within a service using different keys and security levels.

Quick facts about the Octopus card

- 19 million Octopus cards and accessories in circulation
- 50,000 Octopus readers deployed
- 2,000 Merchant locations
- 95% of Hong Kong residents between ages 16-65 use Octopus
- 10 million transactions per day processed
- HK$90 million (US$11.6 million) processed each day

© 2009 Blackboard Inc.

Marketplace advantages

FeliCa is a key technology around which the international standard, ISO/IEC 18092, was designed. The standard defines operation for Near Field Communication (NFC), the technology that is guiding the next generation of contactless technologies.

The NFC standard is compliant with the major contactless technology standard called ISO 14443 but it also has advantages not found in traditional contactless systems. In addition to the reader/writer mode that offers normal contactless operation with ISO 14443 Type A, ISO 14443 Type B and FeliCa cards, NFC enables peer-to-peer and card emulation modes.

Peer-to-peer mode enables two NFC devices to communicate with each other directly. Imagine two NFC phones passing contact information, digital photos or a ticket for an upcoming football game.

Card emulation mode enables one NFC device to act like a traditional contactless card when presented to another NFC device. Virtually any payment or access transaction could one day be conducted via the student ID card or an NFC phone.

As a core component of the NFC specification, FeliCa is in an ideal position to enable its issuers to capitalize on the cost efficiencies that will come from this broader, more open contactless standard. As well, FeliCa and NFC are at the foundation of a form factor revolution that has contactless cards, tokens and mobile phones working together seamlessly as identity, security and payment tools.

In Japan, a hugely successful electronic payment offering has capitalized on its use of FeliCa technology to launch from card to mobile phone payments. The Edy payment system enables prepaid transactions at 137,000 stores and nearly 7000 websites. In addition to the 49 million Edy cardholders, 9 million people are now using Edy to make payments using the FeliCa technology in their mobile handsets.

FeliCa is the world's second most widely used contactless technology. It trails only Europe's Mifare offering in terms of number of chips deployed. More importantly, however, it is the world's leader in secure microprocessor contactless technology. FeliCa is at the heart of many of the most successful and heralded contactless programs around the globe.

FeliCa is extremely reliable and has a proven track record of successful, secure utilization.

One of the longest running and most successful contactless projects to date is Hong Kong's Octopus Card program. Launched in 1997, the Octopus Card began as a fare collection and ticketing alternative for Hong Kong's public transportation systems. Today Octopus is the dominant payment method in transit and has expanded to enable payments at merchant and retail locations throughout the territory.

FeliCa Advantages

- Standardized in ISO/IEC 18092
- Communication speeds of 212 Kbps and 424 Kbps as compared to most contactless technologies that operate at 106 Kbps
- Entire transactions can be conducted in .1 seconds including card detection, mutual authentication, read and write
- Enables multiple services on the card to have individual security keys to protect various areas
- Enables multiple services (up to 8) to be authenticated through a single mutual authentication process to uphold security while increasing speed
- Extremely flexible file structure with ability to control access levels to various services and even to functions within a service (e.g. view balance, decrement balance, increase balance) using different keys and security levels
- Uses fault-tolerant Manchester encoding rather than non-return-to-zero (NRZ) encoding which is more error prone when faced with interference or noise in during transmission

Blackboard transact™

Locations

Worldwide Headquarters

650 Massachusetts Avenue NW
6th Floor
Washington DC 20001-3796
+1.800.424.9299, ext. 4
+1.202.463.4860, ext. 4

Phoenix Office

22601 North 19th Avenue
Suite 200
Phoenix, AZ 85027
+1.800.528.0465
+1.800.476.1400

© 2009 Blackboard Inc.

Blackboard

Blackboard transact™

Your campus. Connected.

Blackboard is your Contactless partner.

Contactless technology is the secure choice for campus card and transaction systems today. Blackboard Transact is leading the way to the contactless campus increasing security and convenience for students and staff while improving the institution's return on investment.

This paper is an initial exploration into how Blackboard Transact can help advance your campus transaction system as your contactless partner.

To find out more, visit:
blackboard.com/contactless or call **(800) 424-9299, ext. 4**.

Blackboard