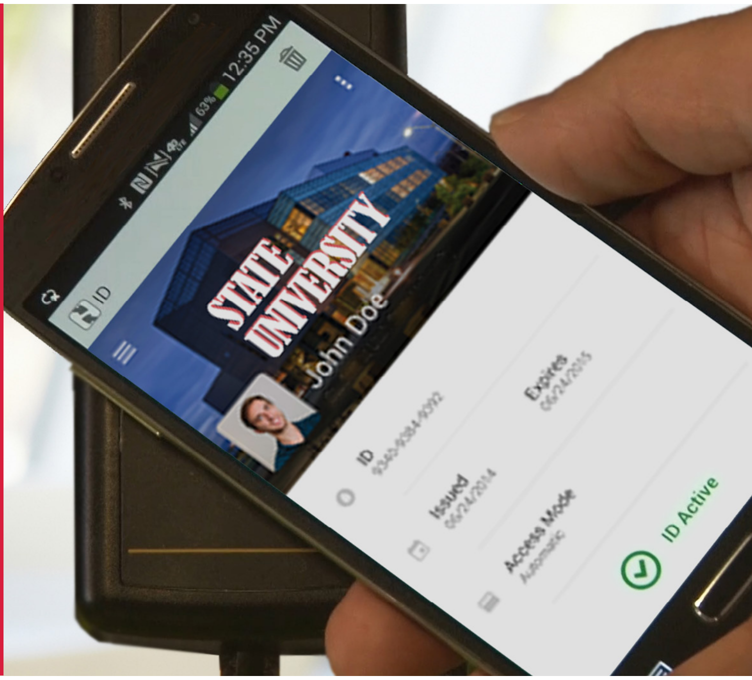
Blackboardtransact™

Best Practices for Migrating to NFC-Enabled Contactless Technology

Today's campus IDs serve as a multi-functional credential giving students the ability to access their dorms, make on- and off-campus purchases, receive their financial aid disbursement electronically, attend ticketed events, and even get their printing, copying, and laundry done and paid for.



> **"We saw Blackboard's Contactless solution as a way for us to keep pace with rapidly-changing technology by adopting a solution based on industry standards."**
>
> **Nirmal Palliyaguru**
> **Director of ACCESS and Conference Services**

Campus credentials and their various uses represent a rapidly-expanding technology aiding campuses in operating more efficiently while enhancing the student experience. Today, traditional magnetic stripe and prox cards—once the standard with any campus commerce or security deployment—are being replaced in favor of more sophisticated and secure NFC-enabled contactless cards and smart phones.

How Contactless Works

Contactless identification credentials contain a computer chip with a connected antenna, enabling credentials to communicate with a reader over a wireless interface. The term "contactless" comes from the fact that the credential and reader don't need to physically touch during operation—rather, data is shared between the two by a process known as radio frequency (RF) communication.

Sharing data via RF communication is extremely common. In addition to AM and FM radio signals, RF communication makes possible many modern conveniences 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, both the sender and receiver rely on their own power supply.

Contactless cards, however, don't 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.

Contactless Card Security

Encryption

All communications between a card and reader are encrypted. This renders attacks based on eavesdropping 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. In addition to the transmission being encrypted, the actual data on the chip is also encrypted using similar methodology, providing an additional layer of security.

Mutual Authentication

Two parties—a credential and a reader—are involved in every contactless transaction. From a security perspective, it's crucial cards only share data with authorized readers, and that readers only process transactions from valid cards.

This is ensured through a cryptographic process known as mutual authentication, in which the card and reader independently verify the authenticity of the other before initiating a transaction.

The key benefit of mutual authentication is 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.

Why Contactless?

Security, engagement, and innovation are staples for universities in student recruitment and retention. Implementing an NFC-enabled contactless credential on campus helps you lead in those very areas.

› **93%:** High school students who say campus technology is important in their college selection[1]

› **86%:** Parents who believe that the safety of the campus is an important factor in choosing a college[2]

› **80%:** Students who feel a sense of engagement and connection to their campus community have an 80% higher chance of persisting[3]

› **42.5%:** Students who select a school based on a campus visit[4]

› **70%:** Students who rated campus security as very important in their college decision[1]

In addition, with more security, greater functionality, and multi-application support, your institution makes ample future-forward technology strides.

The term "contactless" comes from the fact that the credential and reader don't need to physically touch during operation—data is shared between the two by a process known as radio frequency (RF) communication.

Getting Started with Your Contactless Conversion

❶ Determine which contactless technology fits best for your campus.

Blackboard developed its support for contactless credentials with an overarching mandate to support the international standard for Near Field Communications (NFC, ISO 18092). Blackboard supports three contactless technologies that fall under the NFC standard: Mifare Classic, Mifare Desfire EV1, and SONY FeliCa.

There are important factors to consider when evaluating these technologies, and a university must determine which of these factors is most important.

Security

All contactless cards are exponentially more secure than the standard magnetic stripe and prox cards most schools have typically deployed. However, security and encryption among the options is not entirely equal. Security for contactless technology can be thought of in terms of good, better, and best options. Of the contactless formats supported by Blackboard, SONY FeliCa is considered the most secure, having obtained an EAL 6+ Common Criteria Certification. Desfire, with an EAL 4+ certification, is also a very secure product and provides much of the same security features as FeliCa.

Interoperability

Interoperability refers to the credential's integration and interaction with third-party applications and hardware. Mifare Desfire is best-suited for interoperability due to its flexible file format and broad integration across third party devices. Mifare Classic is also widely accepted on third-party readers; however, its fixed file structure requires greater advance planning when adding third-party applications.

Benefits of Contactless Card Technology

- **More Secure:** Convert to a higher-security, NFC-enabled credential to replace existing, dated mag stripe or prox technology which lacks any security.
- **Greater Functionality:** In addition to access control, allow for contactless payments at all Blackboard readers, including vending, point of sale, and laundry.
- **Lower Cost:** Get more functionality at a lower per-credential cost compared to prox cards.
- **Multi-Application Support:** Host multiple applications on the card.
- **Larger Memory & Read/Write Capability:** Contactless cards can store data equivalent to 100 times that of prox cards and other ID technologies. The data can also be dynamic over the life of the credential, with data being written and re-written to the chip over time.
- **Increased Convenience:** Consumers enjoy the transaction speed of contactless technology and appreciate maintaining possession of their card during a transaction.
- **Future Protection:** Build the foundation for supporting an NFC-based mobile credential.

	SONY FeliCa	Mifare Classic	DESFire EV1
ISO Standard	ISO 14443-C (compatible with ISO 18092)	ISO 14443-A	ISO 14443-A
Minimum Blackboard Transact Version Required	3.x	3.10	3.10.2
Frequency	13.56 MHz	13.56 MHz	13.56 MHz
Speed	212 kbps	106 kbps	up to 848 kbps
Memory Size 4k	1k and 4k	2k, 4k, and 8k	
Application Areas	12	16 to 40	Varies
Read/Write Capability	R/W	R/W	R/W
Read Range	Up to 3 inches	Up to 3 inches	Up to 3 inches
File System	Fixed	Fixed	Flexible
Cryptography	3 DES (AES)	Crypto 1	3 DES (AES)
Evaluation Assurance Level (EAL) Common Criteria Certification	EAL 6+	N/A	EAL 4+

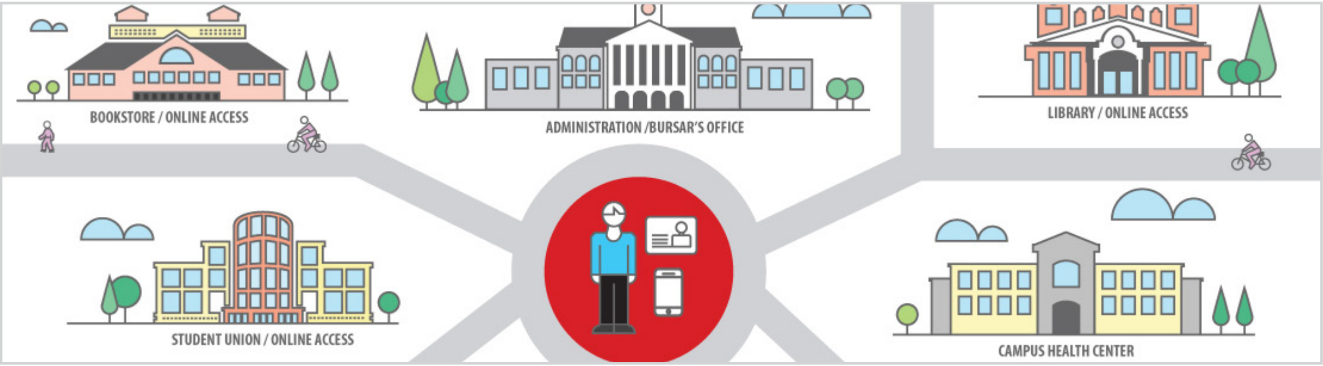
❷ Assess which campus systems will be impacted.

Identifying the systems and readers you expect the new contactless credential to interact with is key in determining credential requirements and card issuance processes. System examples:

- Blackboard Transact
- Third-Party Access Control System
- Parking, Transit

Most system providers use their own private encryption keys/applications. Some system providers only read a Card Serial Number (CSN), which is a non-secure transaction. Blackboard enables schools to capture this data during card issuance, but does not facilitate any transactions via this method due to the security vulnerability.

A one-step issuance process, allowing the card to be read across campus/platforms, is key to ensuring the best student experience. For clients using a third party for door access, Blackboard has created configuration software (Bb Contactless Configuration Manager) that allows you to install Blackboard readers at the edge and communicate with your existing third-party access control system.


BOOKSTORE / ONLINE ACCESS
ADMINISTRATION /BURSAR'S OFFICE
LIBRARY / ONLINE ACCESS
STUDENT UNION / ONLINE ACCESS
CAMPUS HEALTH CENTER

Use of the Campus Credential is Multi-Functional

❸ Develop a card issuance process following best practices.

For your contactless credential issuance, Blackboard recommends the use of a credential desktop printer for personalization including printing of appropriate data elements on the face of the card, encoding the magnetic stripe (if applicable), and writing the various application data elements to the contactless chip. Cards programmed with the Blackboard data/application will only be read by Blackboard-enabled contactless readers.

Next, enable encoding of third-party applications to share data sets with other systems. Use the shared application's default encryption keys (recommended), or a custom encryption key designated by the university, to allow the credential to be used across system providers.

Please note the second application/data set will be placed on the chip in a ASCII format and is required to be a track 2 data-like string (i.e., not a prox format).

Any application data not written to the chip in the initial issuance step must be written to the chip in a secondary issuance process. This can typically be accomplished using a simple USB-type reader/writer connected to a workstation. Refer to third-party application support for specific guidance on the type of hardware required for this issuance step.

Best Practices for Contactless Card Issuance

1. Adopt an ISO numbering scheme using a 16-digit card format with a 6-digit IIN registered with ANSI.
2. Redesign/rebrand your card art and program materials to denote new functionality and leading technology. Blackboard's campus card services are a great choice to help you with this process.
3. Consider using Blackboard's Recarding Services to efficiently personalize your new card stock with current card holder information.
4. Review card art and card handling guidelines prior to creating new card art.

Primary Issuance Pre-printed cards loaded in hopper	Blackboard Secondary Issuance Blackboard Transact server & MF4100	Third-Party Issuance Presented to reader/writer at workstation
› Encodes contactless chip with as many applications as feasible in a single pass › Personalizes front and back of the card › Encodes magnetic stripe (if applicable)	› Encodes contactless chip with Blackboard application as needed › Alternative to issuing via desktop printer › Does not encode Blackboard shared application	› Encodes contactless chip with third-party applications › Repeated for as many third-party applications as required

Card Design Considerations

When purchasing new card stock, Blackboard strongly recommends that the card is pre-printed with the background elements. With this method, only personalization data such as the cardholder photo, name, etc. are printed on the card when it's issued on campus. Purchasing pre-printed card stock provides the most professional finish and also minimizes the chance of having surface imperfections resulting from the embedded chip, sometimes caused by card designs.

Purchasing pre-printed card stock provides the most professional finish and also minimizes the chance of having surface imperfections resulting from the embedded chip, sometimes caused by card designs.

General Card Design Considerations

- A white background gives a professional appearance, and is most likely to yield successful printing results.
- When a colored background is used, allow ample space to accommodate a white "knockout" for placement of the cardholder photo. An optimal size for a photo box is 25mm high by 20mm wide.
- A very dark colored background can often hinder the readability of black-printed cardholder information. As an example, avoid background colors such as Navy Blue.
- Printing white text on a colored background during student personalization is not feasible.
- It's recommended to always place a protective overlay, such as a laminate, on the card after printing student data elements.
- Within your card design, allow plenty of space for cardholder data to be printed on the card.
- Prior to finalizing card art designs, print test cards and be prepared to make adjustments as needed.

Contactless Card Additional Design Considerations

- Avoid large areas with solid color backgrounds—they are more likely to reveal embedded technology.
- Do not place critical elements such as a logo or a photo over the placement of the chip.
- When using a desktop printer, it's strongly recommended to not print any colors or design elements on the area of the card containing the chip. Printing over the chip on a desktop printer will likely result in printing imperfections and could potentially damage the chip.
- When printing over the chip is absolutely necessary, use art with a varied color pattern to make embedded components less obvious.
- Avoid color halftones, particularly grey. They are especially prone to visual artifacts due to card surface variations and printer limitations.

Santa Clara University Case Study

As with many colleges and universities today, data and physical security at Santa Clara University has taken on a heightened sense of importance. Keeping their students safe is paramount to university administrators. That's why Santa Clara—when facing the prospect of issuing new ID cards to its entire campus—decided to make an investment in the future with contactless technology from Blackboard.

"Santa Clara University is in the Silicon Valley and I think it goes with the territory of being in the Silicon Valley as to how we use and promote technology to enhance campus security and student life," said Nirmal Palliyaguru, Director of ACCESS and Conference Services. "We saw Blackboard's Contactless solution as a way for us to keep pace with rapidly-changing technology by adopting a solution based on industry standards. We knew that Blackboard Transact would not only help us solve today's challenge of increasing data security, but also help us establish a base from which we could expand the platform in years to come."

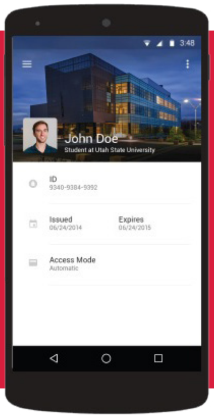
> **"We saw Blackboard's Contactless solution as a way for us to keep pace with rapidly-changing technology by adopting a solution based on industry standards. We knew that Blackboard Transact would not only help us solve today's challenge of increasing data security, but also help us establish a base from which we could expand the platform in years to come."**

Santa Clara's initial foray into contactless has included the reissuing of more than 15,000 contactless ID cards to students, faculty, and staff that are enabled with FeliCa contactless technology in addition to a traditional magnetic stripe on the back of the card. In order to accelerate adoption of the contactless functionality as quickly as possible, Santa Clara outfitted point-of-sale registers in seven existing campus restaurants with contactless readers.

Santa Clara's campus card system is used across campus for everything from dining and bookstore purchases, laundry and copy, off campus merchant management, and door access control. With point-of-sale registers already outfitted to process transactions via contactless, Santa Clara plans to next address door access and vending on campus.

About Santa Clara University

Santa Clara University, a comprehensive Jesuit, Catholic university located 40 miles south of San Francisco in California's Silicon Valley, offers its nearly 9,000 students rigorous undergraduate curricula in arts and sciences, business, and engineering, plus masters and law degrees, and engineering Ph.D.s. Distinguished nationally by one of the highest graduation rates among all U.S. masters universities, California's oldest operating higher-education institution demonstrates faith-inspired values of ethics and social justice.



John Doe
Student at Utah State University

ID
9340-9384-9392

Issued
06/24/2014

Expires
06/24/2015

Access Mode
Automatic

Today, traditional magnetic stripe and prox cards—once the standard with any campus commerce or security deployment—are being replaced in favor of more sophisticated and secure NFC-enabled contactless cards and smart phones.

Give Your Students a More Secure Credential Now

While a campus-wide initiative to migrate to an NFC-enabled contactless card or mobile device requires thoughtful planning, involvement of cross-functional leaders, and changes to your overall credential program, the heightened security, greater interoperability, and innovative boost that your campus benefits from make it well worth the conversion. A solid partner with a wealth of experience and demonstrated successful processes can make it even more effective and easier to achieve your goals.

About Blackboard Transact

Blackboard Transact delivers the security and convenience of a single, unified credential that not only meets your campus needs, but transforms your students' overall campus experience. It provides unified security, disbursement, and transaction solutions—from building access and online financial aid disbursement to campus meal program management and on-and off-campus purchasing. Plus, Blackboard Transact provides round-the-clock services and online training. For more information, visit http://transact.blackboard.com/contactlessbestpractices.

[1] *CDW-G 21st Century Classroom Report*

[2] *CampusExplorer.com. (n.d.). http://www. campusexplorer.com/college-advice-tips/3C268085/Campus-Safety/. Retrieved 06 15, 2013, from www.campusexplorer.com: http://www.campusexplorer.com/college-advice-tips/3C268085/Campus-Safety/*

[3] *Noel-Levitz Research – Mid-Year Retention Indicators Report: https://www.noellevitz.com/documents/shared/Papers_and_Research/2011/2011MIDYEARINDICATORSREPORT.pdf*

[4] *UCLA Study: The American Freshman: National Norms Fall 2011*

transact.blackboard.com/contactlessbestpractices