IDENTIV WHITE PAPER

Identity Verification Solutions for Safe, Secure Learning Environments

Over 19.4 million students attended colleges and universities in the fall of 2020 in the United States. More than two million new students join these institutions every year, and almost as many become alumni annually, creating a fluid student lifecycle.

Campus security is at the forefront of all higher education institutions. The sheer number of students entering and leaving a facility is one of the compelling factors in keeping campuses safe.

With these changing roles and cycles, higher education environments must deploy and maintain a robust physical access control system (PACS) to keep track of new identities and roles for campus security.

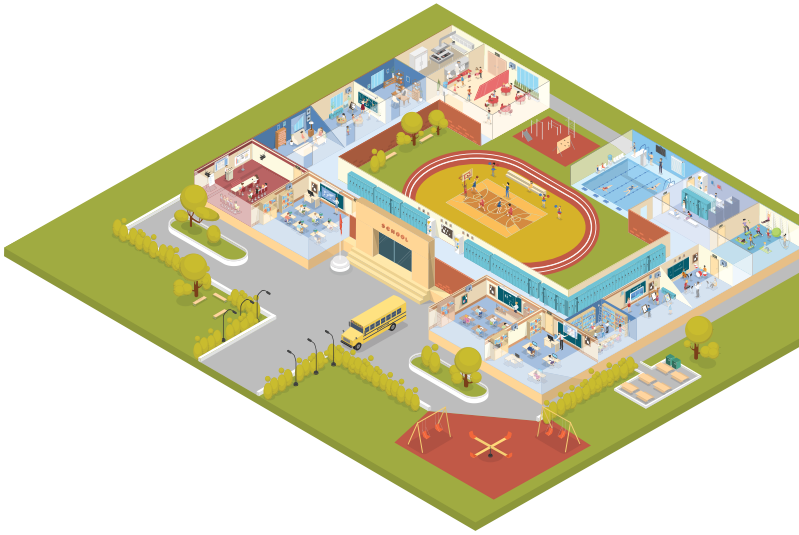
State of Campus Security

Higher education facilities see high traffic volumes every day from staff, visitors, and students. This makes them a soft target for multiple crimes, including theft, vandalism, and assault. Modern campuses install a variety of security systems and surveillance cameras which, in some cases, are enough to deter a crime. At minimum, these end-to-end systems make it easier to identify perpetrators.

Campus populations are easing back into their classrooms, and the spotlight is shifting back to U.S. campus security. Though the country has made significant progress with laws such as the Clery Act, universities have the power to ensure students and staff are safe on campus and in dorm rooms by taking security a step further with identity verification and access control.

With the threat of COVID-19 and concern over similar future scenarios, the demand for contactless physical access control in higher education has also grown. During the past two years, campuses responded to the need for contactless solutions without compromising security by identifying access control systems enabling touchless verification.

Many universities and colleges are adopting smart card credentials for access control. Smart cards can integrate with legacy systems, but using smart card technology also provides the added benefits of encrypted data to protect sensitive information and memory options to support the use of multiple applications. .



Campuses must work towards adopting modern access control technology to provide the most positive experience for students and staff while maintaining the highest levels of security at their facilities. Highly secure smart cards and multi-technology physical access control readers are the future of maintaining a safe learning environment for campus communities.

These changes should include implementing mobile-based credentials to keep up with the evolving expectations of learners. With more than 81% of Americans using smartphones today, a mobile-based access control system can be used across multiple applications, including cashless vending, library, printing, school notification apps, cafeteria transactions, and accessing on-campus transportation.

Mobile solutions are easy to implement and are also a cost-effective way for students to access various services and locations on the campus via the same credential they use to access other academic-related functions, like communicating with professors, checking their grades, or registering for classes.

The Campus Card

The campus card, or student ID, is an identification document first developed in the 1990s to provide access to various services for college and university students. Until recently, campus card applications were limited to access services such as borrowing books, accessing school amenities reserved for students, and attending school events.

Identification is the most basic function of a campus card and its importance has grown exponentially in recent years thanks to the changing security landscape in universities and colleges. Colleges and university staff use the same type of IDs to access various facilities in the institution and verify their identities.

The most common cards used for security in colleges and universities include:

Magnetic Stripe Cards: Magnetic stripe cards use a similar magnetic strip to that found on a credit card. They are also an older, lower security form of identification technology as they are easy to duplicate. These are often single application cards.

Proximity Cards: These are low-frequency (LF) credentials based on legacy card technology. They are easier to duplicate and a less secure access control solution.

Smart Cards: Proximity and magnetic stripe cards use legacy technology and provide minimal security to universities. While they are still in use in some higher education environments, they are increasingly being replaced with high-frequency (HF) smart cards.

HF smart cards were developed with high security in mind, specifically in making them harder to duplicate. They contain an embedded integrated circuit that allows for read and write capabilities. They can be used for multiple applications including identity verification, access control, cashless vending, and resource access.

Mobile Access Solutions: In today's digitally centric world, college students are carrying less and less in their bags and most have a mobile device on them at all times. This is driving the adoption of mobile credentials to gain access to various activities and locations within a campus.

Most mobile access solutions use near field communication (NFC) and/or Bluetooth (BLE) technology to allow access. In addition to security, mobile solutions are less expensive to implement by reducing the demand for printing materials and card management. Maintaining legacy systems requires investment in printing equipment and material. It also requires repeating the card generation process when a campus wants to add applications to the cards. Mobile credentials provide higher learning institutions with flexibility when amending permissions in case a card is lost or a student/employee leaves the school.

Biometrics: Biometric access control is gaining traction across the world but only a few universities have some form of biometric access control system. Biometric systems are used in applications such as safeguarding high-security environments like labs. These solutions are still limited in application, especially due to the high implementation, deployment, and maintenance costs.

Role of Identity Verification in Campus Security

The education ecosystem is fluid, from new students leaving or joining schools to more recent shifts in virtual and hybrid learning environments. These changes mean institutions must adapt quickly to ensure students and staff in virtual or in-person environments are as safe as possible.

Highly secure identity verification communicates to campus security teams who the individuals are that access facilities and whether they are supposed to be on campus.

Here are the roles identity verification plays in schools offering higher education:

Better Security

Identity verification ensures all people moving through or present within a campus are securely identified. Security teams must have real-time visibility into who belongs on the campus or has access rights to be on that campus at any time.

Smart cards and readers can be used alongside surveillance cameras to monitor access points and respond to security incidents.

Access control credentials that cannot be duplicated make it easier for campuses to maintain security when a student or staff member leaves the school. With physical keys and even LF proximity cards, some employees or students may make duplicates, leaving the school at an elevated security risk.

Smart cards paired with a highly secure PACS allow schools to give and cancel access to staff and students in real time.

Improved Surveillance

Campuses are highly populated ecosystems with thousands of students likely to be found in one location at a given time, making it a challenge to physically assess every person.

Wearable IDs allow campus security personnel to quickly spot approved visitors or people who do not belong on the campus.

Personal Data Protection

With advances in technology, more schools are adopting smart school IDs. These cards feature an encrypted chip with information only accessible when the chip is securely read. This creates a layer of security for student and staff personal data.

Better Management of Access Points

Schools with multiple access points experience challenges in monitoring all entries simultaneously, forcing them to prioritize high-risk areas and leave other entry points vulnerable.

Deploying an access control system strengthens security and simplifies identity management at schools. Smart cards allow staff and students to only access the buildings and facilities they have permission to access.

Use Cases for Campus Access Control

Physical access control determines who has permission to enter certain areas of a higher education campus. Access control allows different levels of entry/exit:

- Individual access to a single room
- Departmental access to all areas within a particular department
- Outside door access
- Building access

Building Access

Students, staff, and visitors must have IDs to verify they are who they say they are before entering a building. Building access control systems limit the people who can access certain areas of a building.

For example, in areas where only management staff is allowed, access and restrictions are managed within the access control system. When a credential is securely read by a reader, the information is sent to the head end system where access is either granted or denied based on access rights for the card holder. Some verification systems combine this with biometrics to prevent unauthorized access when someone fraudulently obtains an ID belonging to another person.

Vending

Today's smart cards incorporate payment capabilities into the same identification credential. This means students can now verify their identity and use the same card to conveniently make purchases at vending machines throughout a campus.

These vending machines are integrated with a software system allowing them to accept payments from students.

Cafeteria and Point of Sale (POS)

Implementing access control in cafeterias and at point of sale (POS) systems allows colleges and universities to authenticate staff members. Security teams can identify the people who work inside these stations to provide additional visibility into the activities occurring.

An access control system also prevents theft and burglary by employees and outsiders since the system will not admit anyone without the right credentials and keeps a trail of anyone who accesses certain areas.

Emergency Response Access

A good access control system keeps out unwanted people while allowing those inside the campus to leave in case of an emergency. The system must also allow first responders and emergency services to access the facility, even in the case of a lockdown.

Best Practices for Access Control in Higher Education

Effective, comprehensive campus security must include a robust access control system.

Physical access control implies securing each point of entry into a higher education campus.

Some of the best practices to ensure highly secure physical access control on campuses include:

- Setting up clear and distinct perimeters with designated entry and exit points, including inside and outside the school buildings, and assets within the school buildings

- Enhancing entryway visibility by clearing any shadows, landscaping, and obstacles, giving campus security personnel clear visibility of potential threats while deterring criminal activity
- Establishing a well-defined entry route with signage and walkways to prevent accidental unauthorized access into a controlled area

Challenges in Access Control

Parents, students, and stakeholders expect schools to be safe environments for learning. Colleges and universities are responsible for safeguarding their facilities, ensuring they keep their students and staff protected from internal and external security threats.

Physical access control is a necessary security practice, ensuring campuses monitor who enters the grounds or any of the facilities within the school.

Cost

Cost is a major consideration for higher education environments aiming to improve their access control systems to enhance campus security. These cost considerations are greater when a campus still relies on legacy security systems that could be outdated.

In addition to the systems themselves, schools must invest in a team responsible for managing access control technology and initiatives to ensure the university or college remains a safe learning environment.

Schools also face dwindling budgets, a major obstacle for institutions wanting to optimize access control initiatives.

Privacy and Compliance

In adopting access control solutions requiring student private information, schools must also be aware of the related state and federal privacy laws to ensure they protect students' sensitive data.

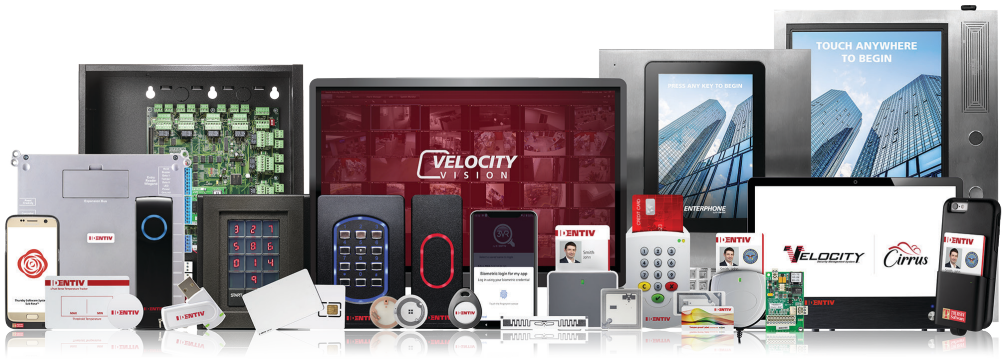
Universities and colleges must also maintain a balance between security and freedom. The goal of implementing an access control system should be to ensure the right people are in the right places at all times, not to add an extra burden to staff and students.

- **The need for integrated solutions:** Implementing an access control solution requires multiple technologies to be successful. For instance, smart cards require access readers for them to work. They also need a database to store the information to verify credentials from various students and staff.
- **The need for flexibility:** Tied closely to cost is the need for colleges and universities to implement access control solutions that can adapt to changes in technology. Security is constantly evolving, and it is easy for education environments to fall behind.
- **Challenges in determining authorization measures:** The goal of access control is to limit who can access certain locations or information within the campus. It can be challenging for schools to continuously determine when to change certain permissions and who to allow in certain places.

Identiv's Identity Verification Solutions for Higher Education Facilities

Identiv offers budget friendly end-to-end security solutions for education institutions to deploy access control and campus security. Identiv's integrated technology provides campuses with:

- Access control solutions throughout college or university facilities
- Continuous monitoring and control of all entry points in every building
- Integration with various campus databases
- Support for one-card systems
- Radio frequency identification (RFID) library and document solutions
- No-touch frictionless credentials that can be read through ultra-high frequency (UHF) technology for hands-free access
- Touchless and mobile campus physical access readers allowing students and staff to hygienically access campus facilities



uTrust TS Cards

uTrust TS Cards are high-security credentials designed for physical access control. They are based on NXP® MIFARE DESFire HF 13.56 MHz technology boasting the highest level of security attestation. uTrust TS migration cards are also compatible with 125 kHz low-frequency (LF) proximity card systems, making it an easy-to-deploy solution in legacy campus environments.

The cards are pre-programmed with a set of diverse keys to protect against unauthorized access. Schools can customize the cryptographic keys on the cards to prevent issues such as forgery and duplication.

High-security uTrust TS Cards are a cost-effective way for higher education institutions to deal with evolving security needs and meet compatibility with existing PACS. The cards are priced considerably lower than existing HF and LF solutions, making it an affordable solution for campus security.

Other benefits include:

- Open design based on industry-standard MIFARE DESFire technology providing campuses with high security assurance and seamless integration with other third-party products
- Customization allowing campuses to utilize a variety of card data formats to match existing infrastructure

uTrust UHF Credentials

Frictionless, batteryless uTrust UHF Credentials feature ultra-high frequency technology making them ideal for identity verification applications that require long-distance reading. Identiv offers two types of uTrust UHF Credentials:

- ISO PVC UHF LF Card
- ISO PVC UHF DESFire EV2 2K Card

uTrust UHF Credentials are a powerful, cost-effective solution with 18-20 feet of long-distance read. The cards are highly compatible with other UHF readers and are based on EPC Class-1 Generation-2 and ISO/IEC 12000-6C standards.

UHF technology can be read through badge holders, handbags, pockets, and backpacks. Versatile uTrust UHF utilizes RFID for access control and identification. Use cases include:

- Providing students and staff with cafeteria access
- Physical access control when entering a building
- Parking lot access

MobilisID

MobilisID is a smart mobile physical access solution designed to provide frictionless access control without students or staff needing to present a credential. It is a cloud-managed solution tapping into the proliferation of smartphones to provide secure mobile credentials to students and staff across colleges and universities.

MobilisID requires the user to download the MobilisID app and wave their hand near a reader to access various locations and facilities in a school. As a touchless solution, MobilisID fits in with the growing need for touchless and contactless integrations intensified by COVID-19.

Both Android and Apple users can store their credentials on the MobilisID app. Whenever they need to access a location in college facilities, they can use Bluetooth-powered MobilisID Readers to transmit their credentials.

The cloud-based portal allows admins and operators to issue, update, and remove user credentials as needed, making it easier and more cost-effective given the size of the university or college population.

MobilisID also eliminates the need for creating or replacing physical credentials for staff and students.

uTrust TS Reader Family

Identiv's uTrust TS Reader family consists of robust reader solutions designed to support all major credentials including legacy proximity, and smart card credentials. These readers come with multiple security layers using the EAL 5+ certified Secure Access Module (SAM).

All security keys are stored in a SAM with any changes and updates signed and validated to preserve the integrity of the system.

uTrust TS Readers are highly flexible, allowing schools deploying the technology to expand or reduce their operations conveniently.

Access Control for a Safe Learning Environment

Access control is a vital part of the security ecosystem that creates a safe learning environment on any type of campus.

It ensures only the right people with authorized credentials are allowed inside a school's buildings, facilities, and events.

Schools have various access control solutions to choose from, but smart cards paired with highly secure physical access readers provide the most robust security. Smart cards also enable the use of multiple applications, including vending, cafeteria, and emergency services.

Identiv works with colleges and universities of all sizes, helping teams improve campus security as they implement and deploy an end-to-end physical access control system. Identiv's solutions are built with security, affordability, and compatibility in mind, empowering higher education facilities to take charge of security on their campus.

To learn more, call +1 888.809.8880, contact sales@identiv.com, visit identiv.com, or book a site walk with a team of experts today.