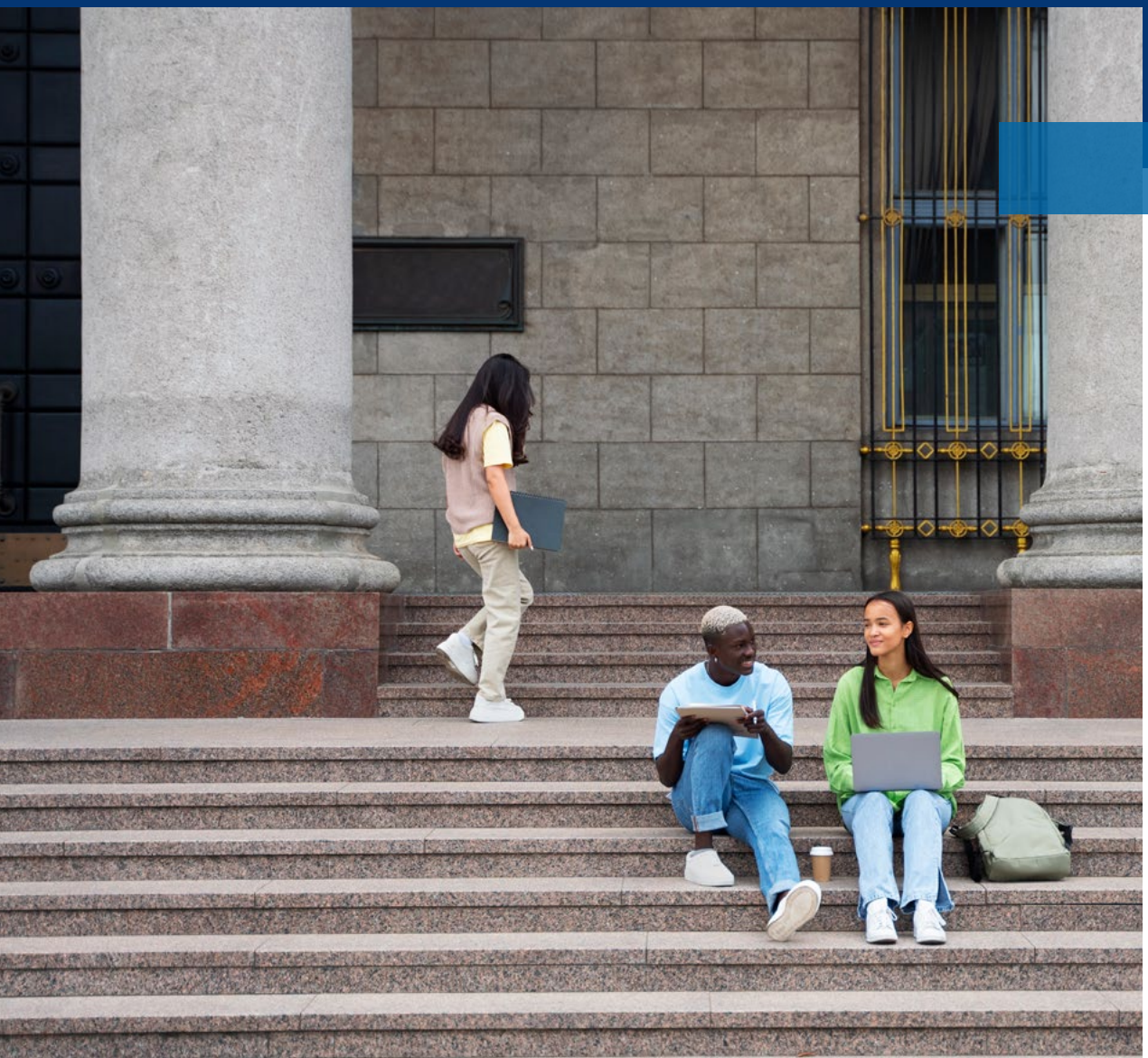
princeton IDENTITY

WHITEPAPER

CAMPUS CREDENTIALS IN A DIGITAL AGE

Meeting Gen Z Students in Their Comfort Zone With Biometric Identity Solutions



INTRODUCTION

19% OF STUDENTS LOSE THEIR ID CARDS EVERY YEAR. AMERICAN COLLEGES REPLACE 3.8 MILLION CARDS ANNUALLY, COSTING $83.6 MILLION

Robust student identity platforms are central to the operations of higher-ed institutions. Their campuses are dynamic ecosystems with thousands, if not tens of thousands, of students demanding seamless access to classrooms, residence halls, transportation, dining, laundry facilities, labs, sporting events, exams, healthcare, and more. As students go about their daily routine, they repeatedly verify their identity to engage in each activity – riding a bus, entering their dorm, buying lunch, or registering for a class. When identity verification is cumbersome or inconvenient, it tarnishes the campus experience. Students without their ID can find themselves locked out of their dorm, unable to sit for a final exam, or refused services at the health clinic.

The challenges of managing a campus credentialing system are daunting. Every semester, there is significant turnover as students enroll and others graduate or drop out. Institutions link a trove of highly sensitive personally identifiable information (PII) to student IDs, including social security numbers, bank routing information, and medical records, all of which must be kept secure. Data privacy and storage policies are subject to strict periodic audits.

Adding insult to injury, 19% of students lose their ID cards every year. American colleges replace 3.8 million cards annually, costing $83.6 million.[1] There must be a better way!

[1] https://www.tile.com/blog/the-cost-of-lost-college-id-cards

THE EVOLUTION OF CAMPUS IDENTITY SOLUTIONS

Until 1974, most educational institutions identified students by their social security numbers. To protect students' privacy and reduce the incidence of identity theft, the Family Educational Rights and Privacy Act required schools to change that policy. Instead, institutions began assigning unique student ID numbers to use as the primary key within their databases and appear on student ID cards.

Around the same time, the first installations of electronic access control appeared on college and university campuses. Adding a magnetic stripe to student IDs turned them into access control credentials – a technique first used in 1972 by California State Polytechnic University.[2] However, widespread deployment of electronic access control for student facilities on higher-ed campuses remained uncommon.

By the 1980s, low-frequency proximity chips, cashless payment solutions, and barcode technology had entered the mainstream. Slowly, institutions began taking advantage of these opportunities by integrating them with student credentialing systems. Then, in the early 2000s, with campus shootings on the rise and terrorist threats top-of-mind, higher-ed began investing heavily in security technology. Student IDs became universally intertwined with campuswide access control.

Within the past decade, smartphones have driven the next major transformation of campus identity solutions. Apple and Android phones now make it easy for students on participating campuses to use their digital wallets to store their Student IDs. Instead of presenting a physical card, they can use their phone or watch to interact with access control readers, point-of-sale devices, online test-taking software, and other situations requiring identity verification. In 2021, the University of Alabama became the first school to issue mobile IDs exclusively.[3] The writing is on the wall; plastic student ID cards are on their way out.

This should come as no surprise. Today's students are digital natives. They carry their phones everywhere and expect to use them for everything. They use Apple Pay and Venmo instead of credit cards. They prefer to use digital tickets when attending concerts and sporting events, or when riding public transportation. They use apps to control the smart home technology they encouraged their parents to install. Why should school be any different? Plus, eliminating plastic cards is consistent with Gen Z's commitment to sustainability. Within the US, there are tens of millions of students enrolled in higher-ed. Imagine how many IDs end up in landfills each year.

However, despite all the benefits of mobile IDs, there are situations on campus when students must or would like to be separated from their devices, at least temporarily. For example, instructors may prohibit the presence of cell phones during exams. Students may find them inconvenient when engaging in certain athletic activities. Some coaches are banning the use of phones during games or practices because social media posts disrupt players' concentration and affect their morale. Students sometimes want to "unplug" for a few hours for mental health reasons. And what if a phone needs charging? A dead phone can't open a door or pay for lunch. Neither can a lost phone. A 100% reliance on mobile credentials is unrealistic.

[1] https://www.tile.com/blog/the-cost-of-lost-college-id-cards. [2] Campus card - Wikipedia. [3] Student IDs on iPhone and Apple Watch expand to Canada and more US universities - Apple

ENTER BIOMETRICS

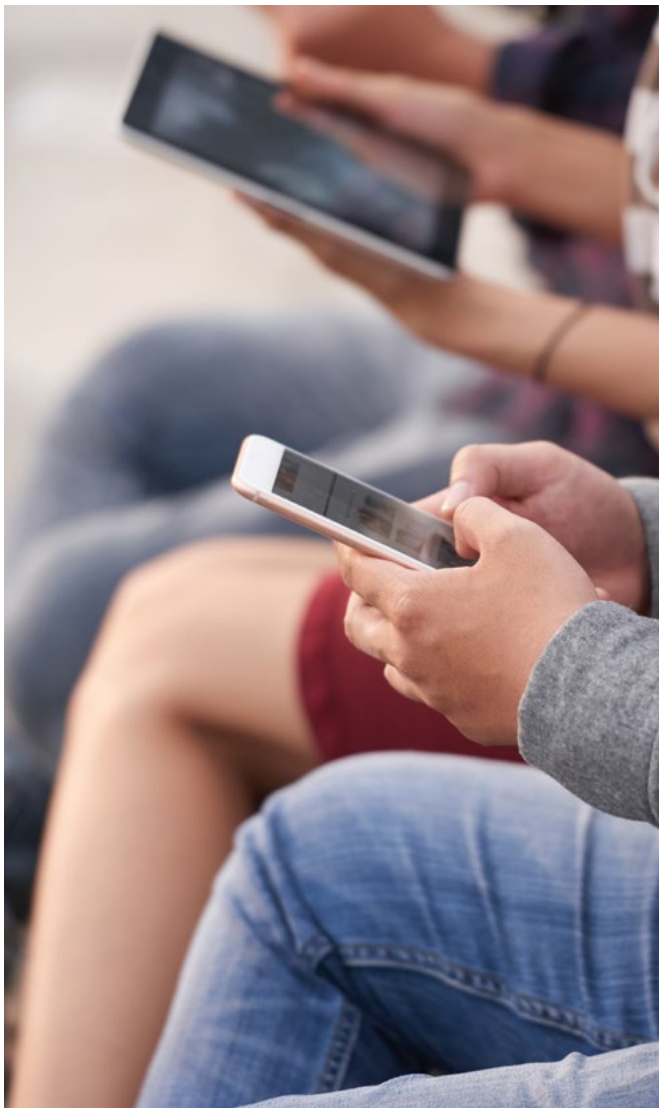
Adding biometrics as part of a campus credentialling platform provides a convenient, highly secure, and flexible means to verify and authenticate student identities. Depending on the application and specific setting, biometric identity technology can be deployed:

- As a choice for students to use instead of presenting a card or phone. Some manufacturers offer solutions that support all three options in a single-reader device.
- In conjunction with other systems for high-security, multimodal authentication.
- In place of a card or mobile reader, for streamlined throughput in high-traffic locations or where other options are impractical.

College-age students overwhelmingly embrace the speed and convenience of biometric identity verification and authentication. 75% of 18-to-34-year-olds use biometrics with at least one app daily.[4] Allowing them to use biometrics on campus in place of cards or phones meets them in their comfort zone.

Of course, no solution is right in all conditions. It's necessary to consider where and how students will interact with the technology. Biometrics are unlikely to replace cards or phones across entire campuses, but they are ideal for some locations. Adding biometric readers to exterior doors of residence halls ensure students never get locked out. Their use in locker rooms and training facilities allows student-athletes to move about freely while wearing pocketless uniforms, swimsuits, or workout gear. Stadiums, theaters, and cafeterias can offer "fast track" lines at entrances and cash registers. High-security areas, like data centers and research labs, can leverage biometrics as part of dual-factor authentication. And, on-campus healthcare facilities can immediately identify patients when they check in for appointments, reducing sign-in paperwork and ensuring accurate record-keeping.

75% OF 18-TO-34-YEAR-OLDS USE BIOMETRICS WITH AT LEAST ONE APP DAILY. ALLOWING THEM TO USE BIOMETRICS ON CAMPUS IN PLACE OF CARDS OR PHONES MEETS THEM IN THEIR COMFORT ZONE.



[4] https://www.biometricupdate.com/202211/gen-z-and-millennials-adoption-of-face-biometrics-reaches-75-percent-report

LEARNING FROM INDIA

Colleges and universities in India are making biometric identity solutions a cornerstone of their attendance systems, as mandated by the country's higher education department.[5] Upon entering classrooms, biometric readers verify the identity of students and faculty and log their presence.

As a result:

1. **Professors can save valuable class time by no longer taking attendance manually.**
2. **Students cannot send someone else in their place for lectures or exams.**
3. **Consistent, accurate record-keeping helps faculty identify chronic student absenteeism and initiate interventions.**
4. **Professors are motivated to arrive on time for class.**
5. **Lecturers cannot impersonate other lecturers.**

While cultural norms in the United States and Canada make it unlikely that higher-ed faculty will agree to allow their employers to monitor their attendance, there is certainly a need for better accountability of students. The frequency of online cheating has increased 14-fold compared to the 15 months before the pandemic.[6] Confirmed incidents include students attempting to take tests on behalf of classmates during proctored exams. That could no longer happen with biometric identity solutions in place.

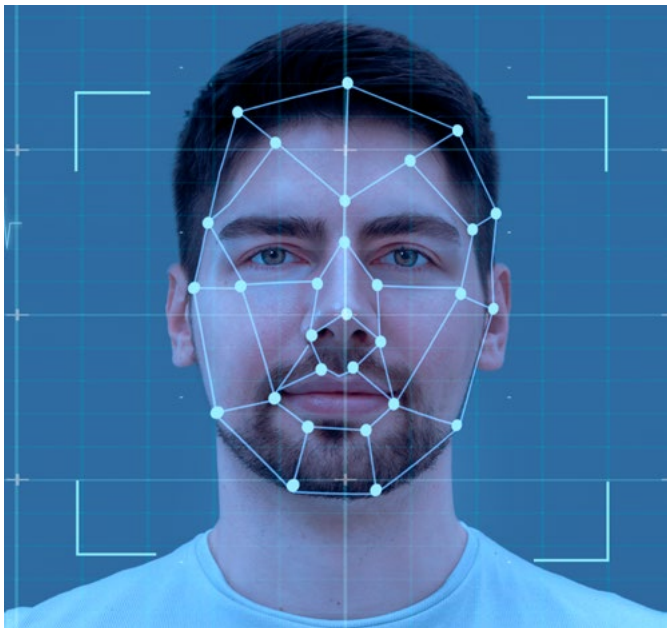
AN ATHLETIC FACILITY GAME-CHANGER

In today's high-security environment, locker rooms must remain locked. From a safety perspective, students – particularly female student-athletes – appreciate knowing nobody can wander in without permission. However, access control on locker room entrances can be anything but convenient. Students may have their hands full of equipment or wear clothing without pockets. If their school relies on mobile credentials, they may prefer to leave their phone safe in their locker while engaging in sports.

Alabama's Auburn University has relied on a biometric identity solution for over a decade to secure its athletic facilities' locker rooms.[7] Rob Stanford, Facilities Management Technology Specialist at Auburn, explains, "When students leave a team or graduate, we just change the permissions and turn off their access. We've had some coaches and students leave and return a few years later. We haven't had to re-enroll them. The system still recognizes them because their eyes don't change. We just reactivate their permissions." The solution can hold and differentiate between thousands of enrollees, including students on the teams, student trainers and managers, coaches, and others with job functions requiring access to regulated areas.

PROTECTING INTELLECTUAL ASSETS

The technology-rich facilities on many university campuses are perfect for conducting academic, commercial, and government-sponsored research. The sensitive experiments and intellectual property housed in laboratories and research centers are targets for tampering and theft. Breaches may occur remotely, over the network, or by someone with physical access to a facility and equipped with a thumb drive or camera. Institutions that fail to keep projects and data secure risk losing lucrative contracts with research partners.



Universities experienced a 44% increase in cyberattacks in 2022 compared to 2021.[8] 99.9% of modern, automated cyberattacks can be blocked through multifactor authentication (MFI). Biometrics are considered the strongest form of authentication, making them ideal for MFI in physical and logical security applications.

[5] https://www.academia.edu/49151863/The_Role_of_Biometrics_in_Higher_Education [6] https://www.insidehighered.com/news/2022/04/28/study-online-exam-cheating

EASE OF DEPLOYMENT

Many of today's biometric identity solutions integrate seamlessly with other security, operations and Point-of-Sale (PoS) platforms thanks to APIs allowing disparate systems to communicate. Schools can preserve the value of existing technology while adding biometric readers to enhance their performance.

Open-platform software makes linking a biometric database with an institution's primary campus identification platform easy, while storing student biometric data within a siloed, secure, encrypted database. Should a network be compromised, there's no risk that a biometric can be reverse-engineered or traced to a student's identity.

Enrolling students is a simple process that any administrator can handle without special technical skills. Some biometric identity solutions even accommodate self-enrollment using the camera on a mobile device.

Biometric solutions may be scaled up over time. Many higher-ed institutions are testing the waters, initially adding biometric readers only at locations with the most urgent requirements to improve safety or convenience. Once installed, most campuses soon add more. A positive response from students, parents, and faculty speeds the adoption of the technology.

CHOOSING A MODALITY

The many flavors of biometric identity solutions are called "modalities." Facial recognition is the most common, but there are all sorts of ways to identify individuals – by their iris, fingerprint, palm, voice, gait, signature, and even ear shape! Post-pandemic, most technology decision-makers will only consider modalities that are part of a contact-free solutions. Nobody wants to place their hands or fingers on a reader touched by countless others.

Other modalities, like voice and gait, are impractical in campus settings. They require too controlled an environment to obtain accurate readings. As a result, modality choices for campus applications tend to be limited to the iris, face, and touchless palm/vein. Of these three, the hands-free nature of face or iris biometrics offers a distinct advantage in terms of convenience.

Environmental conditions must also be considered. Face biometrics are sensitive to light. When the sun casts shadows, the lighting is too dim, or the wind blows hair all over the place, facial recognition accuracy plummets. Hats, scarves, glasses, and masks also impede identification capabilities. Only the iris is impervious to all these conditions. Therefore, it's no surprise that Auburn University, like many other leading institutions, has chosen a biometric solution that uses the iris.

[5] https://f.hubspotusercontent10.net/hubfs/19498362/Documents/Case%20Studies/Princeton%20Identity%20Auburn%20University%20Case%20Study.pdf [6] https://www.infosecurity-magazine.com/news/education-experienced-44-increase/

SUMMARY

Today's higher-ed students crave convenience, speed, ease, and anytime/anywhere access. At the same time, campuses are struggling with expanding operational requirements, shrinking enrollments, greater competition, and tighter budgets. In response, student identity platforms are under scrutiny.

The next few years will prove pivotal as the institutions transition away from plastic and look for ways to meet Gen Z students in their comfort zone – where convenience and sustainability are both highly valued. Integrating biometrics with campus credentialing platforms will deliver on both, while helping institutions remain competitive, improve efficiencies, and increase safety.