The University of Massachusetts (UMass) Boston is Boston's only public research university. It is defined by a deep connection to Boston, a remarkably diverse student body, a focus on ground-breaking research, and an unwavering commitment to student success. As part of the UMass system, UMass Boston combines a small-college experience with the vast resources of a major research university. Spread over 120 urban acres near Boston Harbor, the university contains academic buildings, residential halls, sports, and recreational facilities, plus several administrative and support locations.

The university is home to eight colleges and schools, offering 80+ undergraduate programs (bachelor's degrees, undergraduate certificates, post-baccalaureate certificates) and 110+ graduate programs (master's degrees, doctoral degrees, graduate certificates, and post-masters certificates) to its student body of roughly 16,000 undergraduate and graduate students. Plus, the university employs thousands more faculty, administrators, and support staff.

Securing the Campus

UMass Boston is continuously exploring security products to enhance the safety of its campus, specifically for its students. The primary focus currently is on enhancing access control at residential halls. The university held concerns about implementing a mobile credential system, citing potential privacy breaches and questionable security. They were seeking a solution that would not only protect student privacy but also confirm the identity of the person accessing specific areas.

Traditionally, the university has used physical access cards to manage access to certain buildings. Nevertheless, these cards come with multiple drawbacks. Issues such as lost or stolen IDs are common, which jeopardizes personal identity security; anyone who finds the card could potentially gain access to any building authorized by that card. The situation is further complicated by multiple access points across campus, with varying security levels. Physical access cards can be easily misplaced or stolen. If they fall into the wrong hands, unauthorized individuals could access restricted areas, leading to serious security breaches.

Another significant concern with physical security credentials is "pass-back fraud." This refers to an authorized cardholder accessing a service or area, then passing the card back to another person who now has the same access rights. UMass Boston observed frequent instances of student IDs being used in quick succession in residential halls, dining halls, points of sale, parking garages, and other service points. This indicates potential pass-back and card sharing among the UMass Boston community.

The Solution

UMass Boston and Sentry Enterprises collaborated to enhance the current BeaconCard, to a pioneering self-sovereign identification (SSI) that offers definitive proof of student, staff, or faculty identity for any physical or digital transaction on campus. The university prioritized SSI as it works towards enhancing community members' privacy while elevating security standards. The card's features are only revealed when activated by a valid fingerprint, rendering lost or stolen cards worthless and incapable of unauthorized access or transactions.

The self-sovereign identification BeaconCard is an intricate computing device that securely stores biometric data (fingerprint) on the card itself, not in the university's access control database. A user's fingerprint, which takes about 20 seconds to enroll, is required to activate the card. Without an authorized individual, the card cannot function. Sentry Enterprises' foundation is the SentryCard Identity Ecosystem, which supersedes all existing forms of identification and can be applied to virtually all types of transactions to ensure secure access control.

The new self-sovereign identification BeaconCard enhances security and simplifies processes as the first self-contained, multi-factor biometric credential offering a unified security solution across the UMass Boston campus. The card integrates with existing infrastructure and procedures, eliminating the need for expensive replacements of old systems. Additionally, with biometrics enrolled, stored, and verified solely within the card, it ensures compliance with local, state, and federal privacy regulations.

"The SentryCard promises a significant leap forward in campus security. With its biometric data storage and fingerprint activation, it's not just about access control anymore. Instead, it's about ensuring that the person accessing our campus facilities is indeed who they claim to be. This technology could well be the answer to our concerns about privacy and security. It offers a reliable solution to issues such as lost IDs, unauthorized access, and pass-back fraud. It's a step towards creating a safer, more secure environment for our students and staff."
- Christopher Colon, Director of Student Affairs Technology Services, UMass Boston.

> " The SentryCard promises a significant leap forward in campus security. With its biometric data storage and fingerprint activation, it's not just about access control anymore. Instead, it's about ensuring that the person accessing our campus facilities is indeed who they claim to be. "
>
> -   Christopher Colon, Director of Student Affairs Technology Services

The BeaconCard offers these advantages over traditional physical credentials:

Eliminates card sharing and pass-back. Only biometrically authenticated users can present their BeaconCard in the dining halls and parking garages.	Absolute proof of identity. If the card is lost or stolen, no one else can use it. Biometric proof of identity prevents unauthorized access to residential halls and other sensitive areas.	Enhances privacy for students and faculty. Eliminate the risks associated with biometric authentication by enrolling, storing, and matching the biometric data solely within the ID card itself.	Connects to cash. Areas that use BeaconBucks can verify that the person purchasing is 100% that person. Even if the card is lost or stolen, Beacon Bucks remain secure.	Assists with "healthy campus" initiatives. The student, staff, or faculty member is the only person who needs to touch the card, avoiding hygiene issues from shared touch points.

Roll-out

The university plans to distribute the self-sovereign identification BeaconCard among community members with access to HSC (High-Security Classified) areas before issuing them to incoming 2024 fall resident hall first-year students. The card meets privacy regulations, including the General Data Protection Rights (GDPR), the California Consumer Protection Act (CCPA), and a growing list of biometric information protection acts.

The single card will allow community members access to the main entrances of residential halls and future residence hall rooms. Plans for future usage will include all dining halls, parking garages, library, athletic facilities, vending machines, laundry rooms, technology devices - helping to prevent phishing attacks and other cybersecurity threats.

Wrapping-up

The importance of securing college campuses is paramount; not only does it protect students, staff, and faculty from potential threats, but it also offers peace of mind to those who work and study there. Investing in biometrics is a wise decision for any higher education institution looking to ensure safety and security on its campus. It provides an extra layer of protection that physical access cards and mobile phones can't match.

By taking advantage of biometric access credentials from Sentry Enterprises, UMass Boston can offer its community members a truly self-sovereign identification card, one that enhances security, protects privacy, and offers the university a fast return on investment. Higher education institutions aim to open doors to their communities. UMass Boston and its self-sovereign identification BeaconCard ensures that community members are safe and secure passing through those doors.