

MODERN ACCESS FOR MODERN CAMPUSES

THE FUTURE-READY CAMPUS: UNIFIED ACCESS IN ACTION

Historically, students and staff needed a mix of tools to navigate campus life: physical keys, RFID cards, passwords and PINs, and even cash. Today, expectations have changed; they want one credential—ideally on the smartphone they already carry—to do it all. That’s why many institutions are now looking beyond isolated systems toward unified access: a model where a single credential (physical or mobile) can be used everywhere on campus

By: ELATEC Group
middle-east-info@elatec.com

Alongside their educational mission, universities and schools carry a second responsibility: protecting people, spaces, and data across sprawling, multi-building campuses. User identification and access control are fundamental to campus security, safety, and compliance with privacy regulations. Managing access to classrooms, dorms, labs, lockers, printers, and cafeterias for thousands of users is a daily challenge—one that traditional ID cards and passwords are no longer equipped to handle.

In a recent implementation, more than 150 European educational institutions transitioned to mobile-ready, integrated access systems built around universal RFID reader technology. This example offers a blueprint for how campuses everywhere can modernize authentication without sacrificing flexibility or control.

The Challenge: Securing People, Spaces, and Data in a Complex Campus Environment

Traditionally, physical and digital access systems have operated in silos. A student might use a plastic ID card to enter a building, a physical key to unlock a storage space, a password or PIN to log into campus systems, and cash to make a vending machine or canteen purchase. This frag-



mented approach leads to inefficiencies and security vulnerabilities. It also creates friction for users who must juggle multiple credentials, as well as for administrators responsible for managing and maintaining disparate systems.

At the same time, universities must respond to the rapid rise of mobile credentialing. Students increasingly expect the convenience of using their smartphones to access everything on campus, just as they already do for payments, transit, and entertainment. Digital credentials offer clear advantages: they’re more convenient for users, easier to manage at scale, and reduce the cost and environmental impact of plastic cards.

To meet evolving expectations without

disrupting daily operations, institutions need a way to support both digital and physical credentials during the transition. That means finding flexible solutions that can bridge old and new, creating a path toward modernization without sacrificing continuity or control.

One Credential, Many Applications

As both security expectations and regulatory pressures rise, universities need to rethink how they manage identification and access: not just as a series of isolated tools, but as part of a strategic, campus-wide infrastructure.

The vision behind unified access is simple:



a single credential—physical or mobile—that works everywhere on campus. This approach not only simplifies life for end users but also enables a more efficient, centralized model for administrators and IT. One system, one database, and one set of hardware can now manage access to everything from exterior doors to multi-function printers.

Unified access isn’t just a convenience upgrade; it’s a strategic modernization of campus infrastructure. It creates a more agile, scalable environment that can adapt to changing technologies and user needs. Critically, it reduces operational overhead while enhancing the experience of everyone who lives, learns, or works on campus.

Case Study: Modernizing Access on EU Campuses

A multi-campus access modernization effort in Central Europe offers a real-world example of how universities and schools can streamline campus infrastructure using flexible, mobile-ready technologies. The project began as a pilot initiative to support mobile credentials alongside traditional ID cards across a handful of campuses. It has since grown into a broad deployment, now used at more than 150 educational institutions.

The initiative focused on replacing fragmented legacy systems with a unified



platform for access and credential management. A cloud-based access control solution, provided by Czech systems integrator Etugata, enables centralized control of building entry, lockers, printers, and payment systems. Mobile provisioning is powered by LEGIC Connect through the AliveApp, offering secure mobile credential issuance through smartphones or digital wallets. Students and staff can use their smartphones as access badges via NFC, BLE, or digital wallet integration (Apple Wallet and Google Wallet).

To enable broad compatibility and ease of deployment, the project relied heavily on universal reader technology provided by ELATEC. One key reason: ELATEC’s platform-agnostic architecture supports a wide range of access technologies, making it ideal for complex, mixed environments like university campuses.

At many participating institutions, the existing infrastructure varied significantly, not just in the types of ID cards or mobile credentials in use, but also in the protocols that determine how access devices like readers and controllers communicate and exchange information. These systems often weren’t designed to work together, making it difficult to roll out new capabilities without disrupting what was already in place. To modernize successfully, universities needed a way to bridge across legacy and modern systems, supporting new use cases while preserving compatibility with existing infrastructure. Universal readers from ELATEC provided the technical foundation to unify these disparate systems. Supporting over 60 transponder technologies, 99 physical and digital credential standards, and multiple communication protocols (including legacy protocols like Wiegand and modern, secure protocols like QSDF), the readers ensured that both mobile and physical credentials could be used interchangeably across a range of campus applications. Their versatility allowed Etugata to standardize hardware across access points, from doors and turnstiles to printers, lockers, and canteen systems, without the need for custom development or system overhauls.

Key devices included the TWN4 Slim, a micro-sized reader ideal for tight spaces like printers and lockers, and the Secutos SQ80, a sleek, IP65-rated wall reader built for more demanding physical access points. Both models supported BLE and NFC, enabling mobile credentials through apps or digital wallets while maintaining backward compatibility with existing card-based systems.

The result was a smooth transition path to mobile-first access, allowing institutions to modernize at their own pace while continuing to support current users and infrastructure. Remote configuration and firmware update capabilities simplified rollout and scaling across multiple campuses, while centralized credential management reduced administrative workload for IT teams. The case illustrates how universal readers can serve as the connective tissue in a flexible, future-ready campus access system.

Building the Foundation for the Future of Campus Access

As universities work to modernize their infrastructure for a mobile-native generation, unified access systems built on flexible, future-ready hardware offer a practical and forward-looking path.

Universal readers play a key role in this transition. By supporting a broad range of credential types and communication protocols, they enable institutions to consolidate systems, simplify credential management, and scale access across campus applications without starting over. For students and staff, the result is a smoother, more intuitive campus experience. For IT teams, it’s easier maintenance and greater control.

The European multi-campus project demonstrates how this vision becomes reality. With universal reader technology as the backbone, universities can modernize step by step while maintaining continuity. And the lesson extends far beyond this case: with the right foundation, any institution can create an access environment that is secure and efficient today—and ready for the next generation. ■