

THE DOOR WE LEFT OPEN — THE TRANSFORMATION OF ACCESS CONTROL IN EDUCATIONAL INSTITUTIONS

Jyri Paasonen

The traditional access control solution — a system built with cabling, where every door is connected to a centralized controller — still works in many facilities, but in educational institutions it quickly runs into practical problems.



Tampere Vocational College Tredun manages student and staff access rights on mobile, without separate physical credentials.

A Swedish police chief has been giving the same presentation for several years now. He tours schools, municipal safety events and joint exercises with the authorities, and the core of his message never changes: keep the doors closed and know who is in the building.

This is not a metaphor. He describes, in concrete terms, the difference between a safe school and a school that fails in a serious threat situation.

The audience is rarely surprised by the threat itself. The arresting moment comes when people realize that most schools are unable to put into practice what is being talked about. Not because they wouldn't want to, but because access control was never designed for environments like these.

Traditional access control systems were built for environments where the user base is stable and budgets allow every door to be cabled into a centralized system. Educational institutions are not such environments. That is why a large share of school doors still lack modern access management in practice — not as a conscious decision, but as a consequence of old technology and its cost structure.

In Finland, there is one further particular aspect to the situation. From a legislative point of view, the school principal bears responsibility for the safety of the institution. The responsibility therefore does not rest solely with the municipality, the property company or the service provider.

Security expert Mika Tennberg of Tredun in Tampere sees the change concretely in everyday life. According to him, the safety challenges facing educational institutions have changed significantly in recent years. Schools today offer services such as cafés and beauty care, which increases the number of outside customers in the buildings. At the same time, new access control solutions have to be considered so that outside sources of disruption cannot interfere with teaching.



Mika Tennberg.

Tennberg also points to the rise of alcohol and drug use in the school world, as well as the growth of mental health challenges. For security organizations, these translate into

increasingly difficult situations and disruptions that demand a rapid response. In his view, the behavior of both the institution's own students and outsiders can escalate quickly into violent situations.

Why is traditional access control no longer enough?

Access control is currently going through the same kind of transition that telecommunications and cloud services went through before it. The old infrastructure-centric mindset is colliding with a software-based model.

In a traditional solution the doors are “dumb”, the system is built with cabling, and every door is connected to a centralized controller. Operation often requires servers, maintenance and dedicated specialists. This model still works in many corporate facilities, but in educational institutions it quickly runs into practical problems: excessively high investment costs, slow deployment and poor scalability. This is precisely why a large share of schools' interior doors are still left without access control.

A large share of school doors are still, in practice, without modern access management.

Bitwards CEO Eljas Saastamoinen sums up the problem aptly: the access control industry built its business around infrastructure. Bitwards started from the opposite idea — infrastructure shouldn't be needed at all.

Bitwards is a Finnish digital access management company that develops solutions based on mobile keys and an open platform. The goal is to turn the mobile device into a universal key and to make access management significantly lighter and more flexible to deploy than traditional solutions. Bitwards' solutions are built on an open ecosystem that enables integrations with multiple lock manufacturers as well as security and building management systems.

When the door becomes smart at the factory

In the solutions of new lock manufacturers, intelligence is no longer created at the construction stage but in the product itself. Several manufacturers have brought to market smart lock cases in which mobile opening, digital access rights, local intelligence and traditional mechanical opening are combined in a single product. In practice, this means doors become smart already at the factory.

Traditionally, a door was delivered to the site as a mechanical component, around which access control was built later. Now the lock case itself already contains the necessary technology. On site, the system is simply activated.



Eljas Saastamoinen.

In the Bitwards model, the access right travels in the user's phone. Access rights are managed in a cloud service, while the decision-making itself takes place in the lock's own embedded computer. The technology resembles modern IoT architecture more than traditional access control.

A significant practical difference is that no separate servers, new cabling or heavy controller hardware need to be installed in the building. Installation becomes a software-based deployment.

Educational institutions at the front line of security technology

Educational institutions are one of the best examples of why software-based access management has so quickly become a compelling alternative. Campus environments have large numbers of users: students, staff, visitors, subcontractors, and evening and recreational users. On top of that, access rights change constantly.

Educational institutions are one of the best examples of why software-based access management has quickly become a compelling alternative.

According to Tennberg, it is precisely the sheer number of users and the constant turnover that constitute one of the biggest challenges. Through continuous admission, students begin and complete their studies practically all year round, and not every student can be known personally. At the same time, the open spaces of educational institutions attract outsiders to spend time on campus.

In his view, one phenomenon that matters from a safety perspective is that students and outsiders can be hard to tell apart without visible identifiers. Large student volumes also increase the risk of, for example, drug dealing on campus grounds.

Tampere Vocational College Tredu uses the Securitas Flow mobile access solution, which is based on Bitwards technology. In the solution, the access rights of students and staff are managed on mobile, without separate physical credentials.

Tennberg says Tredu tested several alternatives before settling on the Flow solution. The key reasons were the solution's cost-effectiveness, its integrations with existing locking systems, and the possibility of automating the management of students' access rights.

He considers it particularly significant that students no longer need to be issued separate access credentials. Lost credentials were a constant problem at Tredu. Flow is also integrated with the student information system, so that student data transfers into the system automatically and access rights are generated on the basis of campus data, with no manual work.

Automation, integrations and the future of mobile keys

When the system is integrated with the institution's AD or HR system, a student's or employee's access rights are created automatically as part of normal user management. The user downloads the app, signs in with their school credentials, and their access rights are activated automatically. The entire chain works digitally end to end: identity, access right, mobile key and log data. This improves both information security and data protection at the same time, because access rights data remains under the institution's own control.

According to Tennberg, the use of mobile solutions will grow strongly in the future. In his view, what matters most in a school environment is the system's reliability, its integrations with student information systems, and the automation of routine functions. Access rights should update automatically on the basis of study rights and campus, and when the right to study ends, mobile access should also stop working automatically.

In the future, integrating students' timetables into their access rights may also emerge as a significant direction of development. Although mobile solutions have on the whole been well received, Tennberg also points out practical challenges. On large campuses, finding the right door in the app can take a moment, and phone operating system updates can cause problems. For this reason, easily accessible user support continues to play an important role.

The next phase of access control

Access control is moving into a phase where physical security, identity management and software merge into a single whole. The key change is no longer in the lock itself, but in how access is managed — in real time, centrally, and with software, without physical credentials.

For security industry players, this also means a change in the business model. Value is no longer created solely by hardware and installation, but by integrations, data, continuous services and the ability to manage security as a whole.

At the same time, environments like educational institutions are forcing the industry to solve a question it has long avoided: how can every door be genuinely brought within the scope of control, without costs standing in the way of implementation?

The Swedish police chief's message is, in the end, a very practical one. In school safety, the most important question may also be the simplest: Who is in the building right now?

English translation of the article "Ovi, jonka jätimme auki – kulunvalvonnan murros oppilaitoksissa" by Jyri Paasonen, originally published in Finnish in *Turvallisuus & Riskienhallinta* magazine, issue 3/2026, pages 22–24.