UBISECURE®

intragen
SECURING YOUR IDENTITY

Higher Education and IAM

HOW IDENTITY AND ACCESS MANAGEMENT SOLVES UNIQUE HIGHER EDUCATION CHALLENGES

Intro

With educational institutions worldwide under pressure to offer and maintain secure, compelling digital services, especially due to the rise of online learning since 2020, having a digital-first business strategy is more than just a competitive advantage for educational institutions – it's fundamental. In this whitepaper we'll show how proven Identity and Access Management (IAM) solutions can help streamline inefficient operations and solve unique challenges in the higher education sector.

Challenges

Higher education institutes are facing unique challenges when it comes to managing identities of students, staff and visitors.
These can be categorised as follows:

1. **Ever-changing diverse user base**
2. **Multiple affiliations**
3. **User-friendly services**
4. **Increased security requirements**
5. **Compliance**
6. **Digitalisation**

Let's look at how the correct IAM solution can help in these individual areas.

EVER-CHANGING, DIVERSE USER BASE

Educational institutes have many different groups with different roles accessing their various systems.

- **Students** – across the full identity lifecycle from enrolment, to student, to becoming an alumnus
- **Staff** –regular staff with role-based access to systems
- **Visitors** – visiting lecturers and students, short-term international students, contractors needing temporary access rights

Every year, thousands of new users are onboarded and offboarded, often at short notice. Managing these identities without a dynamic identity management solution means time (and therefore money) wasted on repetitive operational tasks. This can cause serious delays when enrolling new faculty or students, and

ultimately leads to a poor user experience. A good identity management solution simplifies creation, migration and storage of these user identities and ensures a frictionless, any-time, any-place journey throughout their identity lifecycle.

See how Ubisecure and Intragen helped a large university with their IAM objectives in this case study.

MULTIPLE AFFILIATIONS

While students and faculty go through the educational lifecycle, they can have multiple different affiliations (roles). For example, students may work at the university during their studies and end up as an alumnus after graduation. A streamlined IAM solution combines these different roles under a single identity and removes redundant duplicate IDs which can be hard to manage and pose a security risk.

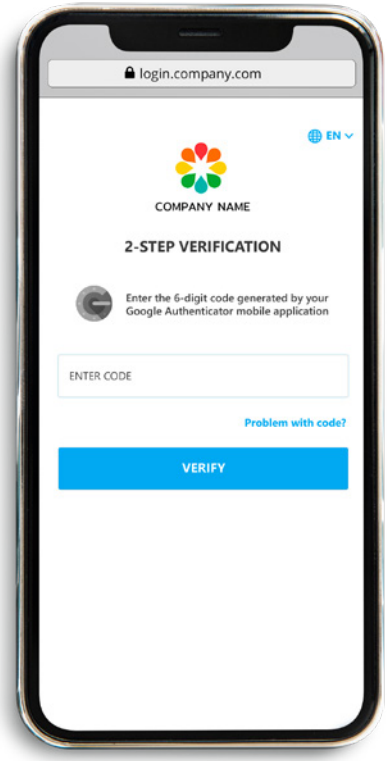
USER-FRIENDLY SERVICES

As well as various user groups, higher education institutes typically have various services. The pressure is on to provide an optimal digital experience as studies now include many digital platforms - such as online classes and content, collaborative tools and other online services. Users have to be able to access all of these services quickly and easily without the need for training or lengthy manual processes.

By enabling **single sign-on** (SSO - a core IAM capability), users can benefit from simplified login to all sigital services and applications using one identity – which would otherwise call for admin-heavy tasks, draining IT support resources. Also by allowing the end user to manage their own accounts and resolve issues themselves, such as passwords or ID management through self-service, the whole process is even quicker and user-friendly. Giving the power to the end user, institutions are able to reduce operational costs and delays significantly, while increasing overall user satisfaction.

Authentication is a critical touchpoint to demonstrate a good user experience. If the IAM platform supports numerous methods to authenticate a user (social, professional, verified and government), organisations are able to choose the best options for their user groups and build good user journeys with the right level of security.

INCREASED SECURITY REQUIREMENTS



Higher education institutes are processing a lot of personally identifiable information (PII), including very sensitive data. At the same time, security issues, such as data breaches, are happening every day. These institutes are a primary target for attacks due to a lack of allocated security resources, limited IT staff and the wide variation in user groups and in their multiple devices. These challenges call for solid security measures.

Multi-factor authentication (MFA) requires more than one identity verification method to gain the user access, including passwords, one-time passwords (OTP) and identity providers (IdPs). Layering access to services with MFA helps secure services and protects (even misplaced) user credentials. Different functions and services might need varying levels of security. By enabling step-up authentication (MFA for only certain resources), organisations are able to have the right level of trust alongside a smooth user journey.

One of the basic principles behind a good IAM system is tying access rights to the identity's permission settings. This increases security as it ensures minimum access necessary to carry out a certain role, reducing breach risk. For example, temporary staff access can be tied to individual contract length. As soon as the contract ends, so does access to all services.

Developing a security strategy based on capabilities such as identity verification, multi-factor authentication and delegated authority reduces security threats and helps to deal with security challenges effectively. A good identity management solution makes sure your users are who they say they are and that they have the right access to only authorised services.

COMPLIANCE

Strict regulations for higher education organisations are there to protect classified data, such as student records. Chief Information Security Officers (CISOs) in higher education may not be experts in the intricacies of regulations such as the General Data Protection Regulation (GDPR), but there are large fines and penalties for non-compliance. Working with an IAM specialist and implementing strong solutions is the easiest way to meet compliance requirements and mitigate the risk of breach and fines.

DIGITAL TRANSFORMATION

Now more than ever, universities need to digitalise to keep pace with competition for international students, remote applications and working or studying from home. Securely authorising and authenticating access from anywhere in the world is an immediate challenge for higher education organisations.

Understanding the relationship between the users in your organisation and where all the data is for those users is the key to success with digital transformation. Identity should never be an afterthought - it should sit at the core of digital transformation and security.

Conclusions

Being digital-first has always been a competitive advantage. As of 2020, it is the key to business success. When selecting an IAM solution provider, it's important to choose a flexible, scalable and robust solution with a skilled integration team that is able to tackle all the unique challenges of higher education.

Ubisecure and **Intragen** are in partnership to provide and integrate an award-winning Identity Platform, to help you achieve your digitalisation goals. This proven IAM solution is designed to increase security and operational efficiency, improve user experience, and comply with regulations – fast.

Ready to get started? **Get in touch!**

About Intragen

Founded in 2006, Intragen has implemented over 125 Identity and Access Management (IAM) projects with a team of experts specifically skilled in identity-led security. Intragen continuously develops its offerings to meet the evolving demands of remote workforces and growing security threats.

About Ubisecure

Ubisecure is a pioneering European b2b and b2c Customer Identity & Access Management (CIAM) software provider and cloud identity services enabler dedicated to helping its customers realise the true potential of digital business. Ubisecure provides a powerful Identity Platform to connect customer digital identities with customer-facing SaaS and enterprise applications in the cloud and on-premise. The platform consists of productised CIAM middleware and API tooling to help connect and enrich strong identity profiles; manage identity usage, authorisation and progressive authentication policies; secure and consolidate identity, privacy and consent data; and streamline identity based workflows and decision delegations. Uniquely, Ubisecure's Identity Platform connects digital services and Identity Providers, such as social networks, mobile networks, banks and governments, to allow Service Providers to use rich, verified identities to create frictionless login, registration and customer engagement while improving privacy and consent around personal data sharing to meet requirements such as GDPR and PSD2.

UBISECURE®

www.ubisecure.com
sales@ubisecure.com

intragen
SECURING YOUR IDENTITY

www.intragen.com
sales-fi@intragen.com