

## IDENTITY ASSURANCE

### Balancing security and cost



#### AT-A-GLANCE

TokenOne enables educational institutions to provide a higher level of security and meet compliance requirements with TokenOne's strong two-factor authentication. TokenOne Authentication replaces multiple passwords and other security technologies with something more secure and more convenient for both the institution and user.

TokenOne's patented next-generation Identity Assurance Platform provides a low cost, easy to deploy, mass-scale solution for:

- Password Replacement
- Soft Token Replacement
- Hard Token Replacement
- SMS Replacement

Discover how TokenOne enables educational institutions to reduce costs, enable compliance and redefine your Identity Assurance expectations by contacting us at [info@tokenone.com](mailto:info@tokenone.com).

#### PROBLEM

Today more than ever protecting the faculty, staff and students as well as a university's assets is a high-profile and complex challenge. With universities further aligning with business for funding and research they cannot afford to leak vital information. Cybercrime is already costing Australian organisations over \$1 billion<sup>1</sup> a year and universities cannot afford to be seen as a 'softer' target.

Traditionally universities and educational institutions are open places for discussion, collaboration and learning which is not only critical to students but also to the faculty and researchers. There is a focus on activities associated with creating, using and sharing information for a university's core teaching, learning and research functions. Add to this the extensive amount of intellectual property (IP) generated by universities, all of which must be protected.

The impact of a breach on an institution is not only reputational but also affects leadership, student learning, wastes vital funds and can lead to a loss of competitive edge in a very tight market.

The frequency and volume of cyber-attacks on Australian universities since 2004 suggest that the confidential data they hold is very valuable to those whose intentions go beyond just identity theft, bribery, malware or internet activism. Most institutions however, do not have the same funds available to them to protect their sensitive information as other large scale businesses. TokenOne provides a patented secure, simple and cost effective technology to protect sensitive information.

#### SOLUTION

TokenOne is an Identity Assurance Platform provider, strengthening authentication by replacing passwords and other security technologies with a single, simple solution which links to risk and identity management systems to provide complete control and non-repudiated secure access. It is easy to provision on and off campus, remotely in Australia or around the world.

TokenOne Authentication enables universities to prove who collaborated on or accessed any document, such as research papers or student essays and reports. TokenOne further enables universities to exceed internal and external expectations with a secure, convenient and cost-effective solution that enables all users (faculty, staff and students) to self manage their own identity and account.

The majority of Australian institutions use Exchange or Office 365 with many ultimately planning to move to Office 365 to increase the ease of collaboration. Engagement in international research collaboration has been a significant focus of Australian institutions that feature in the global university rankings. TokenOne Authentication complements Windows infrastructure, specifically systems currently used to provision and manage their users. This provides an easy and cost effective solution for faculty, staff and students.

This is all achieved with TokenOne's patented technology delivering genuinely strong two-factor authentication that ensures the user's secret PIN is never

1. Norton Report, 2013.

entered, transmitted or stored so is a genuinely kept secret. Many students and staff who already use social networks like Facebook and Twitter will be familiar with the 'notion' of 2FA.

## SECURITY HAS EVOLVED

TokenOne Authentication can assist institutions to address both security and compliance through its low cost, simple to deploy, mass-scale solution that rapidly integrates with existing systems. The TokenOne Identity Assurance Platform does not rely on passwords, eliminating the risks caused by passwords and the high costs of password management. Users only need their mobile device and one solution, not dozens of passwords or other security solutions for multiple accounts and services.

## TOKENONE AUTHENTICATION USE CASES

### PASSWORD REPLACEMENT

Demands for multiple complex passwords are becoming a burden for internal users and students and are also insecure and can be easily hacked. TokenOne provides strong two-factor authentication that is simple and convenient for users and provides security for the university's and the faculty, staff and students' identity protection.

### SOFT TOKEN REPLACEMENT

Soft tokens require yet more passwords and do not prove 'user presence' – only that someone accessed the user's mobile device. TokenOne provides secure, strong two-factor authentication and crucially, the user's PIN is never entered, never transmitted and never stored.

### PHYSICAL OR HARD TOKEN REPLACEMENT

Many public and private institutions have in the past been required to use physical or hard tokens to access sensitive information. These tokens are expensive, inconvenient to carry, complex to manage and do not prove 'user presence'. TokenOne enables hard token replacement with a simple to deploy mass scale solution that is interoperable and will integrate with existing systems rapidly and cost effectively.

### SMS REPLACEMENT

The inherent insecurity and high cost of SMS authentication is driving many to consider alternatives. TokenOne Authentication removes the need for SMS authorisations and enables organisations to prove 'user presence'. Internal users and students are self-supporting during set-up and low administration requirements ensure reduced IT costs.

## BENEFITS

### FOR UNIVERSITIES AND EDUCATION INSTITUTIONS

- Low cost to deploy and manage – rapid Return on Investment and low Total Cost of Ownership
- Meets compliance and governance requirements
- Users self-manage their PIN that can also enable federated access across multiple systems
- Highly scalable, including when users are distributed
- Password management costs, a thing of the past
- Rapid Identity Management (IDM) integration

### FOR FACULTY, STAFF AND STUDENTS

- Highly secure, simple and convenient - one phone, one solution, multiple services
- Self-registration and management with no additional hardware
- Users securely self-manage and self-replace their PIN, even if forgotten
- Increased user confidence as their identity is being protected - their PIN is never entered, transmitted or stored