SECURING BYOD ON CAMPUS AND OFF – WITHOUT AGENTS, TOKENS, OR MODIFYING APPLICATIONS

With mobile devices proliferating the campuses of Australian Universities, and with staff and students expecting access to University information and applications from any device and any location, I.T. security teams need to deploy mobile apps for Android, iOS, and other devices in a way that meets access-security and identity-governance standards. So if you're challenged to deploy native mobile apps to a large user population such as a University, and to tie these identities to University-controlled credentials, this presentation by eB2Bcom will show you the answer: One set of credentials for users and one step to a complete enterprise-grade access solution for mobile devices without the need for rooting the devices, intrusive client software or mobile device management (MDM) tools.

The solutions to be discussed include:

- SSO for native mobile apps, including iOS, Android, and others
- Mobile app to mobile app
- Mobile app to browser-based/SaaS or cloud app
- Federation to SaaS and cloud applications
- Native Two-factor authentication options:
- SMS OTP, Telephony OTP, Email OTP
- Yubikey, Static PIN, Help Desk, CAC/PIV
- Abstraction of authentication code from applications
- Elimination of difficult APIs or calls to implement
- Proven interfaces with existing MDM platforms and network resources such as F5, Juniper and Cisco.
- Self-service user-management tasks, including password reset
- Swift deployment in hours, not weeks.

The presentation will also cover how the identity platform can be extended to include authorisation decisions through the emerging standard of XACML. This is particularly relevant as Universities explore the implications of MOOC – where a resource or application today is accessed by a known and controlled user group, however tomorrow may be accessed by a large external and uncontrolled user base.