ENTERPRISE ARCHITECTURE WITH PLYMOUTH UNIVERSITY

Technology & Information Services

EA-POL-011-Authentication and Authorisation

Author: Paul Ferrier

Date: 07/11/2014

Document Security Level: **PUBLIC**
Document Version: 1.0
Document Ref: EA-POL-011-Authentication and Authorisation
Document Link: http://blogs.plymouth.ac.uk/strategyandarchitecture/wp-content/uploads/sites/4/2014/11/EA-POL-011-Authentication-and-Authorisation.pdf
Review Date: 07/11/2015

EA-POL-011-Authentication and Authorisation

Purpose

The purpose of this policy is to establish and enforce practices for secure communication to university systems and underlying information, thus minimising the risk of information leakage or the compromise of systems. Specifically, this policy deals with the identification and authentication of a given user and whether they are authorised to be able to access the target resource or system itself, this will result in accountability and the non-repudiation of actions that are undertaken.

Audience

This policy applies to all members and partners of Plymouth University who are directly involved in the creation, delivery, support, maintenance or that access any aspect of digital information used for teaching, learning and research within the enterprise architecture and contributing component architectures.

Scope

This policy applies to all systems that contain technology, application and information components throughout the organisation, including hosted or 3rd party platforms, with particular emphasis on public facing, university wide or business critical systems.

Policy

It is recognised that systems located within the University and/or its service provider locations need to be accessed for various reasons, where the classification of information is determined as non-public then an authentication challenge will be provided. This will ensure that the appropriate resources can be accessed by the appropriate individuals in order for them to continue their study, research or carry out their day-to-day work as required. Whilst there are several methods for providing both authentication and authorisation, there is one preferred method that should be utilised within the University's network boundary and this is lightweight directory access protocol (LDAP); alternatively Microsoft's Threat Management Gateway (TMG) may be used to provide disparate web authentication to products or services where LDAP is not a supported authentication methodology.

For systems and services located outside the network boundary federated authentication and authorisation must be prevalent across services for the provision of access control. As a result of this, for systems currently residing outside of the perimeter and any new service Shibboleth (open source federated identity solution) or Microsoft's Active Directory Federation Services are required.

The transmission of user credentials across the University's network boundary must be secured at all times. Utilising the tokenisation afforded by the listed federation services will protect the user account details in transit, due to the trust relationship between on-premise providers and the target systems. Many service providers and solutions look to use lightweight directory access protocol (LDAP) or Secure LDAP to interact with systems on client premises. At the present time, and for the foreseeable future Plymouth University will not support this type of access, all requests to do so will be refused, therefore alternatives should be sought.

The security of authentication data must be tested at regular intervals to ensure satisfactory operation; these tests must be scheduled and communicated with the business in advance to ensure business continuity.

Failure to comply with this policy will lead to the solution architecture being rejected during Enterprise Architecture review, returned for rework, being placed on hold or managed by a waiver to the Enterprise Architecture.

Exception Management

Exceptions to this policy may be granted using the Enterprise Architecture Waiver Process and will be considered on merit as well as alignment with the overall architecture.

Supporting Documentation

This policy is supported by established Enterprise Architecture documents, namely:

- Enterprise Architecture Principles - Principle 6: Common Use Applications
  - "Where appropriate an enterprise single sign-on should be utilized alongside role based access control to maintain data security."
- Enterprise Architecture Principles - Principle 14: Ease of Use
  - "Applications are easy to use. The underlying technology is transparent to users, so they can concentrate on tasks at hand."
- Enterprise Architecture Policy
  - "All Plymouth University information management and technology development, modernisation, enhancement, and acquisitions shall conform to the enterprise architecture and comply with applicable Capital Planning and University budgeting processes. "

Document Control							
Version	**Author**	**Position**	**Details**	**Date/Time**	**Approved by**	**Position**	**Date/Time**
0.9	Paul Ferrier	Enterprise Security Architect	Created the document	13/08/2014	n/a	n/a	n/a
1.0	Paul Ferrier	Enterprise Security Architect	Altered the document for new template	07/11/2014 13:30	Paul Westmore	IT Director	07/11/2014 10:00