Identity Provisioning and Administration
Architecture Proposal

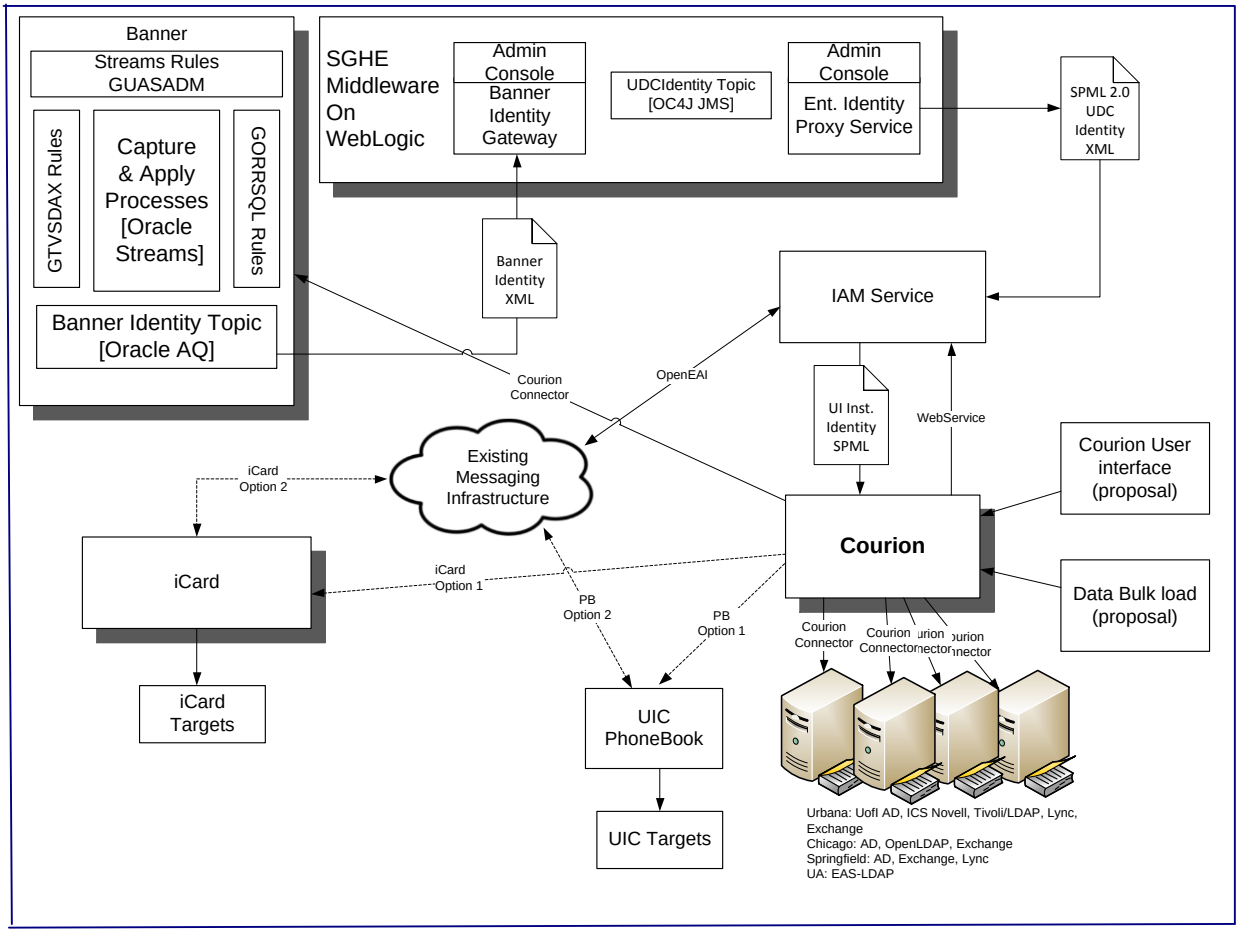
Executive Summary:

This Identity and Access Management (IAM) architecture proposal describes the integration of Courion with the University infrastructure. The primary function of Courion is to serve as an identity vault with rule-based account provisioning capabilities as well as connectors for integrating with downstream systems. Courion is designed to provide an individual with the appropriate access to enterprise systems based on the individual's affiliation with the University (i.e. faculty, staff, or student). It leverages existing authoritative sources to capture, register and assign affiliation types to people. In addition, Courion will provide the necessary tools to manage changes in users access, compliance auditing, roles and other functions related to identity management.

Although this proposal has been discussed with Courion, this document should only be used to facilitate the discussion at the IAMTC and other IAM related committees to help identify the areas of integration between Courion and other systems at the University. Courion will be producing a full design document based on the University requirements, IAMTC input, and the Courion discovery meetings. In this document, the specific implementation and naming conventions of the various components of this design is subject to change based on the underline technology. Significant changes will be brought back to the IAMTC.

The IAM Architecture Proposed Design:

The following diagram describes the proposed initial design of the Identity Provisioning and Administration architecture. Initially, this design will include provisioning to existing campus identity management systems (e.g. Tivioli, Phone Book, etc.). Over time, applications that rely on these systems will be transitioned to Courion and eventually the campus identity systems can be decommissioned.



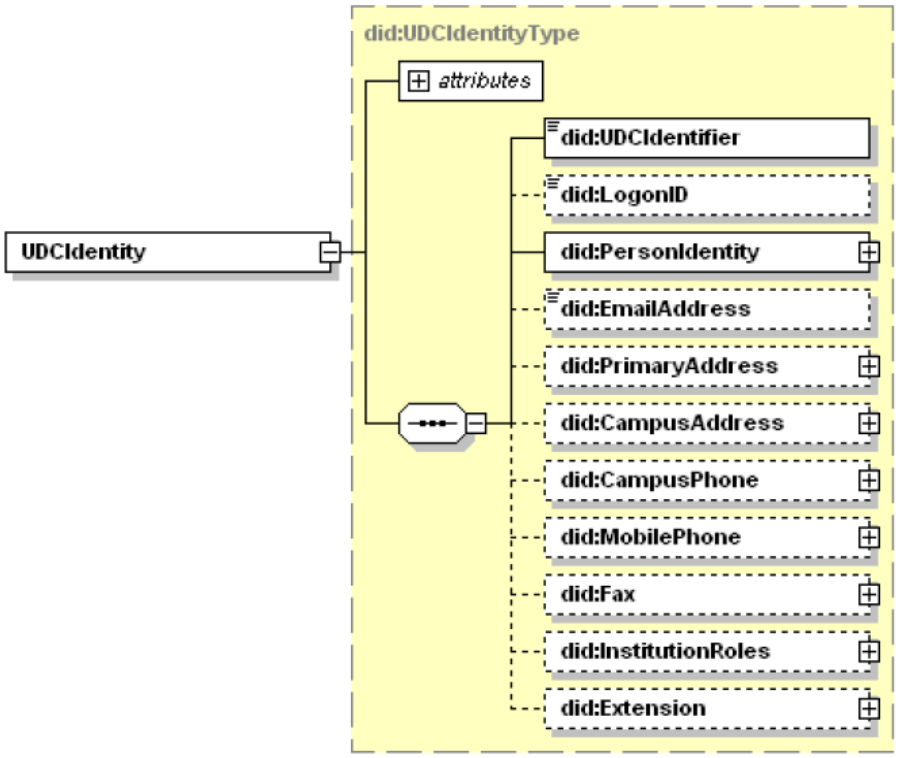
Architecture Components:

Banner:
Banner is the University of Illinois Enterprise Resource Planning (ERP) system. This system is currently the authoritative source for the majority of Identity information for identities associated with the University of Illinois. Banner also implements critical University business processes for managing information related to employees, students, recruits and some vendors. Because of the role of Banner, the Implementation team recommends making Banner an official authoritative source for the ongoing data feed to Courion.

Banner Enterprise Identity Service (BEIS):
A collection of common software components and embedded capabilities in Banner that support the management of Banner identity information. BEIS is able to trigger events in Banner to create, change, and deprovision identities for downstream consumption. BEIS components include:

- Oracle Stream and Oracle Advanced Queuing technology: This technology is deployed in Banner infrastructure to allow for the capture of identity changes in Banner and publishing this data via XML format.
- WebLogic and Proxy Services: Weblogic and Enterprise Identity Proxy Services is used as an XML transport service with transformation and grantee of delivery architecture
- UDC Identity: UDCIdentity is XML structure that collects and packages identity data about a Banner identity. The UDCIdentity XML structure also provides the basis for exchanging user data

between Banner and external provisioning systems such as Courion. The following diagram describes the UDCIdentity data.



IAM Service:

The IAM service will provide the following functions:

- XML Transformation: The IAM Service will consume data from BEIS and transform it to a format that is readable by Courion. During this process, the IAM service could be used to filter data before calling the Courion workflows. It also can be used to make calls to other data sources to include additional pieces of data from other authoritative data sources.
- Additional IAM Service Functions: The IAM Service can be used to, UIN, perform person matching and allow users to create their NetID. Courion has advanced capabilities to generate NetIDs,but currently it does not support users to interactively create their own NetIDs. This function will be available in Courion later in 2013.
- Publish data from Courion: This service can be used to allow the publishing of data from Courion to existing systems via the existing University messaging infrastructure. This option could be used in the initial phases of the IAM project to interact with existing system such as Phone Book, iCard, and other OpenEAI based systems. This is particularly important when bi-directional interaction communication between Courion and other systems is needed.

iCard:

iCard will continue to provide the UIN generation and person matching process during the initial phases of the IAM project. This UIN generation process will be transitioned over time to the IAM Service.

Courion:
This system will implement business rules and processes to manage user registration, access, provisioning, auditing, compliance and other services. Workflows will be developed in Courion to accept data from the IAM Service, register the identities and update and provision/deprovision the target systems. Courion uses Connector technology that was developed specifically to communicate natively with target systems such as Active Directories, LDAPs, Databases, Applications, etc.