Identity Management and Collaboration

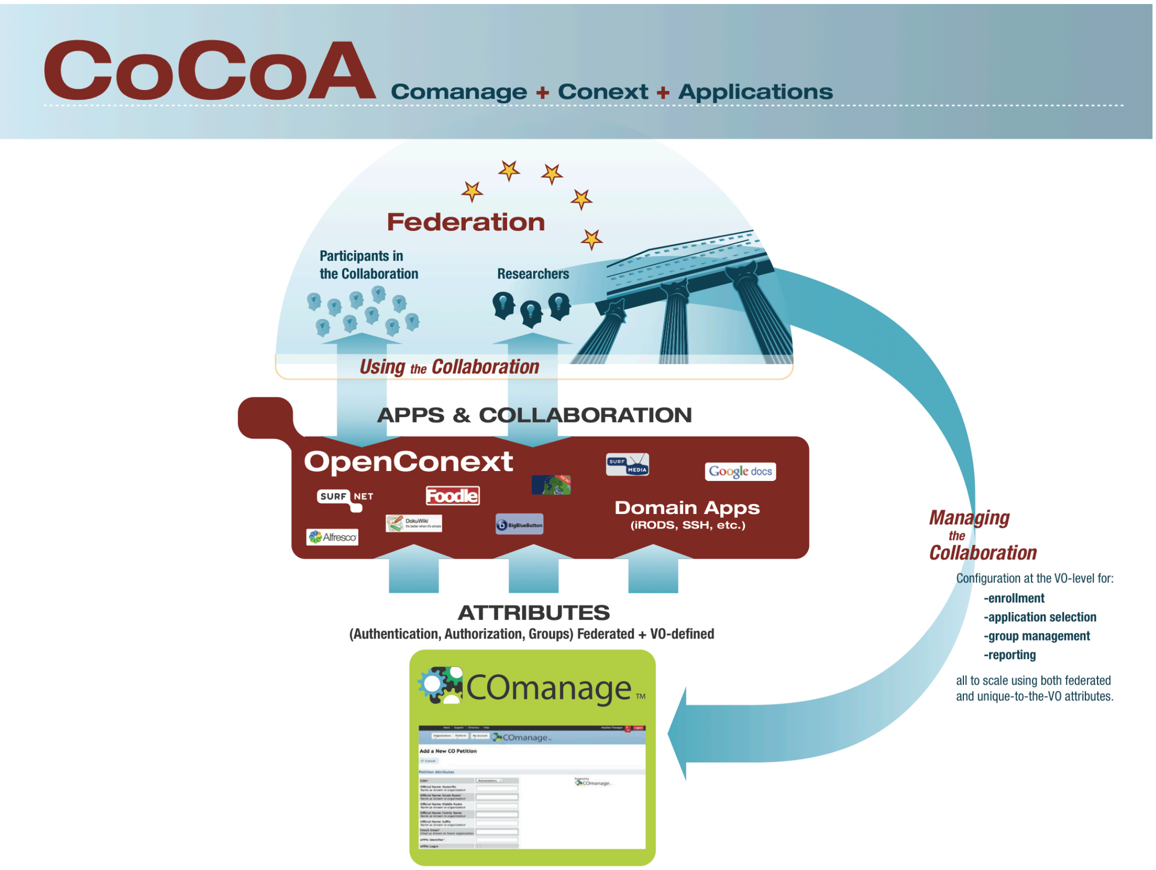
CoCoA
Comanage + Conext + Applications
Federation
Participants in the Collaboration
Researchers
Using the Collaboration
APPS & COLLABORATION
OpenConext
SURF NET
Foodle
DokuWiki
Alfresco
BigBlueButton
SURF MEDIA
Google docs
Domain Apps
(iRODS, SSH, etc.)
ATTRIBUTES
(Authentication, Authorization, Groups) Federated + VO-defined
COmanage
Managing the Collaboration
Configuration at the VO-level for:
-enrollment
-application selection
-group management
-reporting
all to scale using both federated and unique-to-the-VO attributes.

Fig. 1: Conceptual diagram of the CoCoA platform

Collaboration is at the very center of the R&E mission, with inter-institutional and international engagements a very common characteristic. To make such collaborations effective both technically and from a user perspective requires three components:

1. A set of collaboration apps such as wikis, lists, calendaring (ad hoc and event), and conferencing, etc. These applications should have their identity and access needs met through open interfaces (API's, SAML assertions, LDAP, etc.). The use of open protocols allows the focus to be on the community groups and access control that are the payloads of those protocols, and on growing an ever more comprehensive set of domesticated applications. A consistent UI, for the user both as user and as collaboration manager, is also essential.
2. A set of domain tools (computation systems, storage, common scientific analytic tools, databases and data sets, etc.) that also have their identity and access control needs met with open community-standard interfaces. These tools are noteworthy not only for their users - relatively small in number but consequential in importance - but also their requirements: command line applications, process authentication, delegation of authorization needs, etc.
3. A collaboration-centric identity management and access control mechanism that leverages the growing R&E federation infrastructure, gives the collaborators the ability to mingle institutional and collaboration attributes and permissions in order to manage access to collaboration resources, and provides consistent user experiences. While the sciences and domains may be different, and the desired collaboration apps vary (though a core seems to be common to all collaborations) the need to identify participants, to have scalable authentication and authorization across the tools and apps, and to have reliable reporting are the same.

The target collaborations for this work are not social networking nor crowd-sourcing populations, nor is it those enterprises (and perhaps a few virtual organizations (VO's)) that have bricks-and-mortar-and-endowment infrastructure. The intended user community is the formal VO's, with grants and perhaps experimental facilities, less formal VO's, the inter-institutional WG at state, regional and national levels, etc. These tend to be collaborations that are large but not open, that need several forms of access control across a variety of applications as well as a need to manage the lifecycle of participants, privileges and materials. Such activities are legion in the R&E space, and increasingly common in other verticals.

The COmanage Project, a National Science Foundation fully-grant-funded activity within Internet2, is developing tools and resources that allow virtual organizations to meet their research objectives without building their own stand-alone identity management infrastructures. By leveraging external (federated) identity management services and standard group and registry tools, authentication and authorization are handled in a single, efficient process that integrates a mix of collaboration attributes and each member's home organization attributes into all of the various applications that serve a collaboration community. It allows a collaboration to seamlessly use a variety of tools instead of being locked into a proprietary suite. It also allows collaborators to focus on what they do best — advancing scholarship and research in their field of expertise – rather than the complexities of identity management.

OpenConext was developed by SURFnet as part of the SURFworks and GigaPort3 programme. It is an opensource technology stack for creating and running collaboration platforms and creates a powerful front end for users to choose for themselves and their workgroups the right applications for their collaborations. When combined with the COmanage Registry service, collaborations have a complete solution from front to back for identity management and collaboration needs.

COmanage can be thought of as a specialized VO identity management system for VO. The needs of VO are unique in the identity management world, and while there is some overlap with enterprise identity management, a few specialized requirements come in to play:

- A VO will have very specialized attributes and permissions not replicated anywhere else.
- For reasons of sustainability and freshness of data, VO's also want to leverage enterprise attributes.
- A VO will have business processes for participation that feed their onboarding and enrollment that are specific to their collaboration; they have no systems of record to build on, as enterprises do.
- The lifecycle of identities within the collaboration go beyond the lifecycle of identity within a single institution.
- There is no identity management staff to run the systems; there are, at best, general IT architects for the VO who may be uninformed of the modern federated world.

For organizations that want to replace an ad hoc (or largely absent) set of identity management tools within their own cyberinfrastructure, there is the COmanage toolkit. The toolkit can provide a coordinated, federated access control layer to a VO's wiki, list processing, audio conferencing, etc. as well as potentially their specific domain applications. The COmanage toolkit provides a rich set of critical components to a VO, including: an identity registry, automatable processes for enrollment, collaboration identity lifecycle maintenance, group attribute management, and provisioning that developers can connect to the domain science applications in use by the VO. From an end user's perspective, having the COmanage toolkit working behind the scenes allows individuals to create personal groups as well as manage organizational groups that they have permissions for, and allows the user more control over the information they might share within the VO.

Poorly done IdM, with its gaps, frustrations, and spills, takes more time than IdM done structurally. Students enrolled in classes wait for weeks to get to scientific resources. Researchers long gone still have active permissions, creating serious security concerns. Ad hoc agency reporting requirements generate chaotic weeks-long multi-institutional fire. With a platform like CoCoA, these pain points and many others are addressed for VOs and their associated institutions.

Current Status and Project Timeline:

- The first proof of concept for the combined COmanage plus OpenConext platform was demonstrated at the VO Architectural Middleware Planning workshop (VAMP) in September 2012.
- Further progress will be demonstrated at the Internet2 Fall Member Meeting in October 2012.
- The COmanage component of CoCoA is slated for a 1.0 release by the end of 2012.

More information is available online:
COmanage = http://www.internet2.edu/comanage
OpenConext = https://wiki.surfnetlabs.nl/display/OpenConext