

# **Authentication Services Roadmap for Cornell**

v1, September 22, 2005

Cornell Information Technologies, IT Security Office

Authors:

Andrea Beesing

Steve Edgar

Tom Young

# Authentication Services Roadmap for Cornell

<b>Background</b> .....	3
<b>Drivers for Strong Central Authentication</b> .....	3
<b>Current State</b> .....	3
<b>Future Directions</b> .....	4
<i>Increase Methods for Integrating with Central Authentication</i> .....	4
<i>Increase Security of Authentication</i> .....	5
<i>Stronger Authentication Services</i> .....	6
<b>Appendix A: Approved Mechanisms for Interfacing with Cornell’s Central Authentication Service</b> .....	8
<b>Appendix B: Authentication Mechanisms Not Planned for Implementation or Identified for Retirement</b> .....	9

## Background

This roadmap focuses on authentication, the process by which a system, resource, or application verifies the identity of an individual. A related topic, to be treated separately, is authorization, the process by which a system, resource, or application grants a person access to only the resources and information appropriate to the role or status.

Provisioning, or how we manage identities and access privileges as people arrive, depart and change roles, will also be handled in another paper.

## Drivers for Strong Central Authentication

A number of developments are driving colleges and universities to implement and build upon a strong central authentication service. Recent years have seen an increase in legislation and regulatory requirements regarding the release of personal information and managing who has access to certain types of information. An ever growing incidence of identity theft and computer security compromises further increases the potential for the exposure of institutional data to unauthorized individuals. The University's open computing environment adds yet another challenge to the task of securing restricted resources. In addition, federating technologies are being deployed to support sharing of information across institutions using the ID granted by the individual's home institution. Strong authentication is a pre-requisite for entry into such arrangements with external parties.

The University has endorsed the value of a strong central authentication infrastructure by approving the impact statement for the proposed policy, "Authentication of Information Technology Resources." (<http://www.cit.cornell.edu/oit/policy/drafts/AAAis.pdf>) Developing the software to obtain and store passwords is not trivial and once implemented, becomes an attractive target for those intent on gaining access to resources and data for which they are not authorized. Encouraging campus service owners to use the central authentication service whenever possible by providing multiple interfaces for that integration helps reduce the number of "weak links" which can be introduced with separate authentication services. The authentication roadmap developed by the IT Security Office represents a focused effort to balance ease of use and security for services taking advantage of the central authentication service.

## Current State

Kerberos is a secure authentication service that can be deployed over a heterogeneous computing environment such as the one which has evolved at Cornell in response to the needs of faculty, students and staff. One key advantage is the security of user passwords. They are stored in a highly secure (hashed) format on the central server and are not transmitted over the network. Kerberos has been deployed at Cornell for over a dozen years and many business critical applications rely on it for authentication:

(<http://www.cit.cornell.edu/kerberos/AppChartSideCar.html>).

## Authentication Services Roadmap for Cornell

Many applications have no built-in support for Kerberos. Cornell has spent significant resources developing methods for such applications to take advantage of the central authentication service. Implementing and integrating an entirely different solution, including any commercial offering, would come at a significant cost so the benefits would have to justify the change. The Identity Management team will continue to monitor the status of alternate solutions for potential consideration in the long-range future. In the short-term the recommended direction is to continue leveraging the University's considerable investment in the current Kerberos-based infrastructure by providing additional mechanisms for application integration.

Kerberos requires that the software on a user's computer understands this authentication method, and that a Kerberos client is installed on the system. For applications that don't natively support Kerberos, CIT developed SideCar, an "out-of-band" program that can independently communicate with Kerberos. This approach, however, does not work in all network environments (NAT issue) and has some inherent security issues. Moreover, it would be very costly to maintain versions of SideCar for all the different platforms in use at Cornell. The lack of a version for Unix systems has been a source of customer dissatisfaction for some time.

CUWebLogin allows us to provide authentication services using the Kerberos password system without any client software. It represents a trade-off between the very strong security of pure Kerberos, and the need to extend the benefits of central authentication to a wider range of services. CUWebLogin is what we refer to as a "Kerberos proxy." This means that the password is transmitted to the CUWebLogin server in encrypted form (SSL/TLS), and then the CUWebLogin server communicates with the Kerberos server on our behalf. A proxy weakens the security of Kerberos to some degree, since the password exists not only on the client but on the proxy server as well. The risk is mitigated by maintaining the CUWebLogin servers in a highly secure manner.

### **Future Directions**

Over the coming year and beyond, resources will be focused on providing additional means for service providers to interoperate with the central authentication service, while continuing efforts to address known weaknesses. When implementing new infrastructure components, priority will be given to those solutions 1) which extend the benefits of central authentication to applications used campus-wide and/or 2) extend the benefits of central authentication to mission critical applications or to applications providing access to institutional data.

#### *Increase Methods for Integrating with Central Authentication*

Based on the above criteria, the following integration methods will continue to be supported or will be implemented as components of the central authentication service in the short term:

## Authentication Services Roadmap for Cornell

1. Native Kerberos
2. CUWebLogin
3. Active Directory
4. Radius
5. Kerberos proxies for CIT Messaging Services (Email and Newsservice)

If an application is used campus-wide or serves a mission-critical role, and it is feasible to write or modify the application to talk to Kerberos directly, this is the preferred approach. The investment will result in ease of administration and the strongest password security for the users of that application. In the case of open source products, Cornell will be contributing back to that community. New Kerberos proxies will be implemented only after careful review and approval. They must be administered according to established Security Standards for Authentication Servers to mitigate the risk.

Where none of the CIT-delivered solutions are available to an application, local authentication may be required. Separate accounts and passwords will have to be maintained for that application. Instead of investing in proprietary, expensive solutions for these applications, the Identity Management team will work with stakeholders to streamline the processes by which these accounts are established and removed. Potential solutions for this problem will be covered in the IT Security Provisioning Roadmap. For example, better self-service applications for requesting and managing these accounts may address some of the overhead involved in maintaining separate accounts and passwords.

### *Increase Security of Authentication*

Cornell is still using Kerberos version 4. This version of the protocol has security vulnerabilities not present in Kerberos 5. Of most concern for Cornell is the decrease in the strength of the encryption method Kerberos 4 uses (DES), as the machinery capable of breaking it has become more widely available. In addition to the security issue, MIT has announced its intent to drop support for Kerberos 4 in a future release.

Implementing SideCar in version 5 would introduce an unacceptable security vulnerability to the central authentication service. In addition, the need for SideCar has dwindled as web-based applications have increased. For these reasons, we will be retiring SideCar within the near future. This will require working with the owners of services to ensure that they have a plan for eliminating SideCar dependencies.

There are a small number of CIT services that still use clear text passwords to communicate with the central authentication service (Newsservice, FTP access to CU People). The IT Security Office will work with service owners to eliminate this practice as soon as possible.

In the spring of 2005, the IT Security Office implemented password complexity standards for the central authentication service. As new users are issued IDs their passwords will follow these standards. Existing users will be encouraged and eventually directed to choose passwords that comply with the new standards. This effort will result in

## Authentication Services Roadmap for Cornell

passwords which are much more difficult to crack than those adhering to the previous standards.

There will be instances where a service must use local authentication. For those cases, a set of standards is required to govern the level of authentication employed based on the type of data at risk. There are efforts currently under way to work with University data stewards and other stakeholders to develop standards for authentication levels, from level 0 (publicly available) to the highest level for the most sensitive institutional data.

### *Stronger Authentication Services*

Services providing access to some types of institutional data will require even stronger authentication than the NetID and password protection Kerberos offers. Stronger authentication involves multi-factor assurance of identity--something you know such as a password and something you have such as a card or small computer device. A central multi-factor authentication service will co-exist with Kerberos for an as yet undetermined period of time. When specific requirements for multi-factor authentication are clarified by policy and business drivers, implementing a central solution will become a high priority.

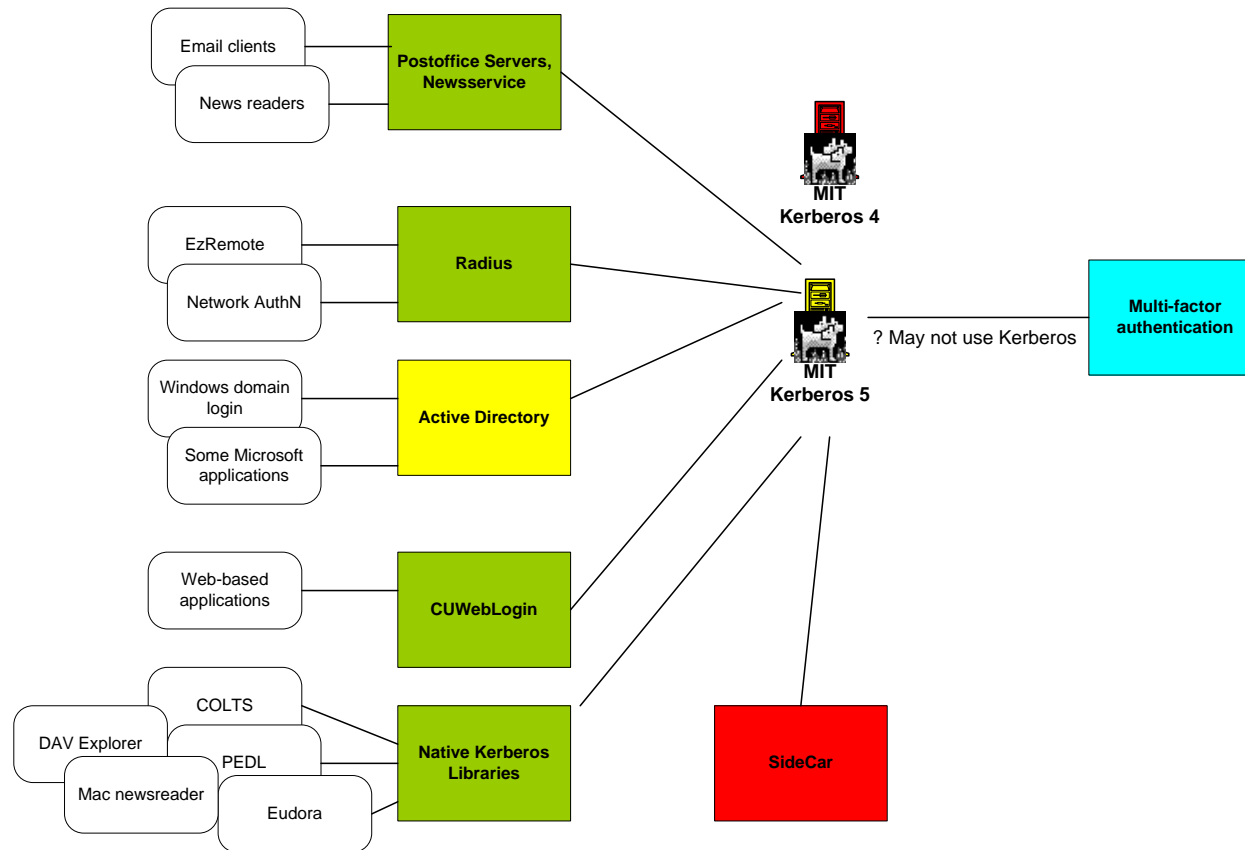
# Authentication Services Roadmap for Cornell

Green - current, will retain

Yellow - planned, schedule to be determined in FY07

Red - current, will retire, schedule to be determined early FY06

Blue - future, no schedule yet



## Appendix A: Approved Mechanisms for Interfacing with Cornell's Central Authentication Service

For a detailed chart of the current state of campus-wide application integration with central authentication see: <http://www.cit.cornell.edu/kerberos/AppChartSideCar.html>

Method	Coverage	Applications that can potentially use this method in future	Timeframe
<p>Native Kerberos</p> <p>Most secure and therefore, preferred where feasible. Password not transmitted over the network.</p>	<p>--Some commercial applications (ex: Eudora)</p> <p>--Netprint for Mac and Unix</p> <p>--Applications programmed in house, using CIT-maintained software libraries (ex: COLTS)</p> <p>--Open Source applications (requires Cornell resource commitment)</p> <p>--Custom solutions such as the desktop proxy suitable for developer use only</p>	<p>--Windows news reader</p> <p>--Oracle Calendar</p> <p>--DAV Explorer</p> <p>--CU People</p> <p>--webMethods</p>	<p>Currently available (CASAPI, Native Kerberos libraries)</p>
<p>CUWebLogin</p> <p>Most preferred for web-based applications. Secure proxy.</p>	<p>--Web-based applications in Unix/Apache and Windows/IIS environments</p> <p>--uPortal</p>	<p>--Kronos</p>	<p>Currently available.</p>
<p>Radius</p> <p>Proxy that provides Kerberos authentication for network access</p>	<p>--Ez Remote</p> <p>--Future network authentication, probably wireless initially based on 802.1x</p>		<p>Radius implementation in place for Ez Remote. Upgrade/replacement may be required for network authentication. Schedule to be determined by NCS.</p>
<p>Active Directory</p> <p>Direct method of Kerberos authentication</p>	<p>--Windows domain login</p> <p>--Some Microsoft applications (Outlook)</p>	<p>--Public lab workstation authentication</p>	<p>FY06 – CIT pilot</p> <p>Schedule to be determined – Campus implementation</p>
<p>Kerberos Proxy</p> <p>Least preferred option due to increased exposure to password and potential for desensitizing user about exercising caution before entering NetID and password in non-standard prompt. Server subject to minimum security standards.</p>	<p>--Central email via TLS</p> <p>--Reset password utility</p> <p>--News service</p>		<p>Implemented after approval by governing body. Criteria to be used: 1) No other alternative available to meet business need, 2) application used campus-wide or deemed mission critical</p>

## Authentication Services Roadmap for Cornell

### Appendix B: Authentication Mechanisms Not Planned for Implementation or Identified for Retirement

Mechanism	Issues
SideCar	<p>Cannot be securely implemented in Kerberos 5. Upgrade from Kerberos 4 to Kerberos 5 must be accomplished in FY06. MIT has announced it will drop support for Kerberos 4 in the near future.</p> <p>Cannot be used behind NATs (network address translator), a network environment common for many off-campus users.</p> <p>Very few campus-wide applications requiring SideCar (most can use either native Kerberos or CUWebLogin)</p>
Proprietary client solution to replace SideCar	<p>Options examined are very expensive to implement and maintain. There are very few campus-wide applications in need of this service, making it difficult to justify the expense of such a solution for a campus-wide deployment. The results of surveys and discussions with the campus community in 2004 showed very little interest or need for this product.</p> <p>CIT has decided to move forward to develop a desktop proxy solution for selected applications used by developers. It has been determined that the time required to develop and support this solution for a limited user base is a worthwhile investment.</p>
LDAP authentication	<p>An LDAP directory can be set up to proxy for Kerberos. Applications written to authenticate to LDAP can then be integrated with the central authentication service without modification. The concern here is that the application server in this scenario becomes yet another proxy. It is possible to steal passwords at the application server. How difficult this is to accomplish varies from easy to challenging, depending on the software and the security on the server. We recommend not implementing an LDAP authentication mechanism at this time, but to reconsider under two scenarios:</p> <ol style="list-style-type: none"> <li>1) If a request for this service is made, it should be reviewed based on the same criteria established for approving other Kerberos proxies</li> <li>2) Once a multi-factor authentication service is in place, consider using LDAP authentication to replace all single-purpose Kerberos proxies (Postoffice servers, Newsservice)</li> </ol>