Overview
I’ve divided the development effort into three phases. First we’ll prepare the Identity Management infrastructure for the move to Kerberos 5. The Identity Management team will do the bulk of it’s software development in this phase.

Next we’ll announce to our stakeholders that we’re ready to begin upgrading campus applications. We’ll provide stakeholders with information, links to our website, and technical support so that they can begin making the transition to Kerberos 5. K4-K5 upgrades will happen according to the various schedules of the teams involved. During this phase the Identity Management team will also upgrade applications to Kerberos 5 (i.e, the NetID activation client).

The final phase of this project will involve monitoring use of Kerberos 4 and the transition to Kerberos 5. Hangers-on will have to be communicated with, cajoled, etc. Eventually, the coast will be clear, and one morning Kerberos will be restarted with K4 support disabled.

Phase 1 – Prepare for Rollout
The Identity Management infrastructure serves as the primary building blocks for Kerberized applications around campus. Before expecting users to upgrade, we need to upgrade our infrastructure. During this phase we will focus our attention on these goals…

- Minimize upgrade hardships for our users. The easier it is for application developers and web admins to make the upgrade, the easier our job will be during the rollout.
- Where possible reduce unneeded home-grown source code that we support. It would be great if we could come out of this project with a net decrease in support requirements. This would give us more time to devote to new projects like Grouper.

Documentation
Before we can expect other groups to plan for the transition, they will need to have the following documentation made available. Since this is required for planning by other groups it will be given the highest priority by our team.

K4 to GSSAPI Cookbook & K4 to K5 Cookbook
The documents will be used by us and other groups as helpful guide for porting from Kerberos 4. The content is in the form of a how-to guide with an emphasis on simplicity and content, not format.

CUKerberos.jar API Manual
The CUKerberos.jar will have new calls added to support Kerberos 5. These calls must be documented along with the existing K4 calls.

KClien32.dll API Manual
The KClien32.dll will have new calls added to support Kerberos 5. These calls must be documented along with the existing K4 calls.

CUWebAuth User Guides
Both the Apache and IIS versions of these documents need to be updated to reflect changes that Kerberos 5 will bring. Most notably, removal of SideCar functionality. Some consideration will be given to possibly rolling the two documents into a single one to decrease maintenance overhead and help reduce the feature drift between the IIS and Apache implementations.
Website
The project website needs to be modified to reflect status and progress throughout the duration of the project. All documents must be made available on our website.

Identity Management Software Changes
Here are the changes to be made, in no particular order.

Update Changes to gssapi.dll
Ideally we will be able to use the vanilla gssapi.dll from MIT. If this isn’t possible, then the changes will need to be updated.

SideCar Macintosh
Will no longer be supported

SideCar Windows
Windows SideCar has some UI functionality in addition to the SideCar CUSSP server function. The same UI features appear to be covered by MIT’s leash program. There should be some research into whether leash will cover our needs. The next version of “SideCar” could be…

- Vanilla Leash
- Leash, with Cornell mods
- Stripped down Sidecar, with all SideCar CUSSP server functions and associated UI removed.

CUKerberos.jar
The java library will have some new calls added to provide support for Kerberos 5. It will also continue to support the existing Kerberos 4 API. Every effort should be made to make the Kerberos 5 calls similar to the Kerberos 4 calls in order to simplify the upgrade path for application developers. By creating a distinct Kerberos 5 API developers can upgrade applications one by one in a controlled manner. Extreme care must be taken not to break existing applications with the new jar, so that IS applications developers can do the upgrade work according to their own schedules.

KClien32.dll
New calls will be developed to support Kerberos 5. However, some consideration should be given to the possibility of retiring KClien32 altogether and replacing calls to KClien32 with MIT calls. This will require identifying all software that makes calls to the KClien32 DLL.

CUSSP Libraries
There are three libraries identified…

- cussplib.v1 – Used by CUWebAuth, CUWebLogin, Permit server, cusspclient command line utility.
- cussplib.v1 (NT) – Used by CUWebAuth Apache/NT
- cussplib.v2 – Used by CUWebAuth IIS and possibly others.

All libraries appear to have Kerberos 5 support. The Kerberos 5 functionality needs to be carefully tested, fixed where broken, implemented where not. Since the NT version of cussplib.v1 is an old branch, some effort should be made to retire it.

CUWebAuth
Both IIS and Apache implementations of CUWebAuth will be modified to use Kerberos 5 calls. Since all implementations depend on the CUSSP libraries, implementation may be gated by CUSSP library implementation. A test plan will be written and both IIS and Apache implementations will be tested according to the plan.

CUWebAuth Usage Tracking
A subsystem will be designed and implemented as part of the CUWebAuth and CUWebLogin daemon that will monitor all deployed instances of CUWebAuth for the following information…
• CUWebAuth Version
• OS and OS Version
• CUWebAuth related server configuration
• Whether SSL is in use
• IP address(es) of server
• Kerberos principal

CUWebAuth will infrequently report this information to cuweblogind, maybe daily. This information will help us track our progress during the upgrade, but it will help long after the upgrade by giving needed information about our users.

CUWebLogin Daemon
The CUWebLogin daemon will be modified to support Kerberos 5. When deployed, the new server will run on a new TCP port so that both the Kerberos 4 and Kerberos 5 services will be available. Eventually the Kerberos 4 server will be removed when no longer in use.

In addition, cuweblogind will have be modified to support CUWebAuth usage tracking. The server will store CUWebAuth usage information in a local database.

CUWebLogin CGI
The CGI provides the login screen that the user sees. Parts of this system will need to be upgraded to use Kerberos 5 instead of 4. Additional UI changes will be required to accommodate the official Cornell web look and feel. Implementation of the Cornell UI will be accomplished with assistance and direction from CSM.

On the login screen, the Help Desk contact information will be replaced with a site specific Help Desk contact. This new contact information will be gathered during the registration of the site (see Self-serve Keytab Registration WebSite).

Permitd
The permit server will be modified to support Kerberos 5. The Kerberos 5 implementation will be deployed on a different TCP port and share the permit database with the Kerberos 4 enabled permitd. This will allow both Kerberos 4 and Kerberos 5 applications to access the permit server.

Depending on the timing, this activity may be implemented while implementing the Permit-to-Grouper bridge. In this case, the Kerberos 5 work will be applied to the bridge code, not the permitd code.

Eventually, the need Kerberos 4 daemon will be shutdown when it is no longer in use.

Self-serve Keytab Registration WebSite
This will involve the design, implementation, and testing of a new website that allows qualified users to generate a Keytab and register CUWebAuth servers. This site will be used to capture information such as the name of the application, the department, and the primary and secondary contact’s e-mail address, root URL for the site if using CUWebAuth.

When considering where to store the registration data, performance should be considered for the following attributes because they are used by CUWebLogin…

- CUWebLogin IP address registration information (currently in DBM)
- CUWebAuth HelpDesk contact and Department (new)

It may be necessary to mirror this data.

Note: naming conventions should steer us away from “-agent” principals so as to ensure retirement of SideCar. This site will also enforce any other new conventions, processes, and policies that may arise (see Process and policy for Keytabs). Any pre-existing principal which
doesn’t follow new conventions will require that a brand new one be created that fits the new conventions. The website should capture the obsolete principal name, so that we can monitor and retire the principal eventually.

**CIT Web pages scrubbing**
CIT web pages need to be scrubbed for mention of SideCar and Kerberos 4 and any other components that are being phased out. This work may take place over the next phase as well, while other groups are upgrading applications.

**Process and policy for Keytabs**
It’s that time. We need to consider things like naming conventions for Keytabs, who can request a Keytab, etc.

**Phase 2 – Campus Rollout**
Here are the development activities during campus rollout.

**Identity Management Activity**
These are activities that are clearly Identity Management’s responsibility. Others may arise.

**ChangePW Application**
Upgrade to support K5, test, deploy.

**NetID Activation Application**
Upgrade to support K5, test, deploy.

**NetAdmin Client**
Upgrade to support K5, test, deploy.

**Technical Support**
Provide support to IS, I&D, ATA, S&O, and the campus in general.

**Campus Applications Upgrade**
We may need to provide extra hand-holding and perhaps to porting ourselves for some campus applications.

**Track ongoing K4 usage**
Begin tracking and communicating with folks to make sure a plan is in place for every application.

**Communications**
Stakeholder communications, meetings, announce., mailings, website, etc.

**Campus Rollout**
This is work that many groups will be involved in. Each group will need to be notified that they need to upgrade. Each group will need to plan and schedule the upgrade. We will need to communicate with these groups so that we understand their plans and can plan accordingly.

**CUWebAuth**
This is the simplest part of the upgrade and involves only minor effort on the part of web application admins. That is, picking up a Keytab at the new self-serve site, and deploying a new version of CUWebAuth.

**Kerberos Applications Upgrade**
This is the more difficult job. Planning will be more complex, and the stragglers will likely come from this group.
Phase 3 – Monitor and Shutdown

Track ongoing K4 usage
We will continue to track usage and communicating with folks and escalate issues as appropriate.

K4 Shutdown
Timing of this will depend on usage, but we will shutdown the permitd’s K4, cuweblogind’s K4, and eventually Kerberos 4 support itself on the KDC.