Why Informatics Cannot Use EASE and the EUCS KDC

Written by Tim Colles and Simon Wilkinson

Last modified on $Date: 2006/03/03 16:33:51 $ by $Author: timc $

A. Why Informatics Cannot Use EASE

Informatics cannot use EASE because we lose single sign-on *AND* it would be necessary to extend Cosign to add cross-realm support (as it currently assumes all credentials are in a single realm) *UNLESS* we put all our users in the EUCS KDC (see below), ie. the EASE Cosign service needs to get tickets for our users from our KDC to proxy on for our own services to be viable.

1. Putting all our users in EASE would require us to use EASE as our primary authentication mechanism and would also mean using the central EUCS KDC. See below for why we can't do this.
2. There are some halfway houses such as just adding all our students to the EUCS KDC or adding all our users but not our service prinicpals to the EUCS KDC. However most of the arguments below still apply in these cases as well.
3. Even with all our users in EASE we would still need to run our own KDC (for service principals) so the management and support cost versus benefit is then in question.
4. If we did put all (or some) of our users in EASE we would need to reimplement some technology at our end. We would need to do an LDAP lookup on login to map a UUN to a principal (LNAME to ANAME in Kerberos terminology) and PAM/Kerberos callouts do exist to support this. We would also need to be able to map the other way (although most of our services already do this). None of this is currently standard configuration although in the future the new DAL (Database Abstraction Layer for Kerberos) has provision to support this scenario. All this reimplementation would require changes to the core Kerberos libraries which are unlikely to be accepted upstream and hence would carry an ongoing support cost.
5. There is little gain to us anyway unless EASE is adapted to support KX509 and/or SPNEGO/Negotiateauth authentication so we preserve single sign-on.
6. We want to extend our own Cosign service so that it has support for SPNEGO/Negotiateauth (so that we can remove KX509 from the chain for desktop login). It would also let us do SSO and delegated credentials

without needing to run KCT on the KDC. EASE would need to be extended in the same way.

7. We provide a means for automated service registration on our Cosign service - such a facility would also need to be added to EASE.
8. We need to consider the management cost of maintaining our own KDC locally (low) together with disadvantages to us of using the central KDC directly (many).

B. Why Informatics Cannot Use The EUCS KDC

1. We have little confidence in the password security of EASE. This is because the initial (default automatically created) passwords remain permanently active even if the user changes their password to something else. These initial passwords are viewable by any CO in the University with IDMS access and access to these passwords allows any of a users other central passwords to be altered at will.
2. An additional concern beyond the above is that originally the initial passwords were not configured in this way and would be changed (and no longer visible) when the user changed their password. However, upper management pushed for the initial password to be retained as it is now for user simplicity. This resulted in the reduced security of the system and this was a decision that was taken without any consultation with the primary service users. See AuthWP mailing list for further discussion on this.
3. The EUCS KDC does not have the `requires_preauth` flag set on any of its user principals. This means that EASE users can't authenticate to any DICE services which have the `requires_preauth` flag set on their service key (by default, this means all DICE services). Not having `requires_preauth` set also opens up EASE accounts to some fairly powerful offline dictionary based attacks.

   Subsequent to this document being written EUCS were contacted regarding this issue. Once the security concerns of not having this set had been noted, they changed their KDC configuration (and the flags on all 45,000 of their principals) to set this attribute.
4. There is no mechanism provided for programmatic entry of principals into the EUCS KDC - for host and per-user instance principals. This is necessary for our automated machine installation for example.
5. EdLAN robustness is an issue - we have slaves at all our sites to protect against network failure. In a recent network situation the EUCS approach was to drop our connectivity to EdLAN until it was resolved. While the EUCS response to this issue is the only realistic approach given current network technologies it means that had we been using the central EUCS KDC the consequence on our users would have been severe (inability to login and use our services which they could quite happily have carried on doing with the current configuration we have).
6. Service development - we tend to be ahead of EUCS and many changes we are already thinking about making in the future will require changes on the central KDC. This includes (but is not limited to) adding

PKCROSS/PKINIT support (integration of a public key infrastructure with Kerberos) and RXGK (adds GSSAPI encryption for AFS volume data which is currently encryptable only with fcrypt which is a reduced 46bit 1des which may be adequate now but won't be in a few years time). There is also an intention to reduce password exposure by looking at moving to hardware tokens and while this may also be something EUCS are considering we are likely to go that way far sooner. In essence the speed of development of services if we used the EUCS KDC is at a rate to satisfy the entire University rather than a rate necessary for ourselves.

7. Source of credentials unclear. For example we have a trust link with the EUCS KDC which means our users can access staffmail easily (and it would make any future move to using that central service more transparent), whereas for Microsoft Exchange authentication is via A/D for which we don't currently have a trust link.
8. Using the central EUCS KDC and EASE for primary authentication takes the reliability of our systems out of our hands. There is for example no Service Level Agreement and no service provision local to our sites (critical given acknowledged EdLAN vulnerability and the EUCS approach to handling such).

C. Integration of Managed Desktop with our AFS Infrastructure

In order to integrate our MDP Windows machines and users into the AFS and Kerberos infrastructure our DICE users benefit from (SSO) and to be able to drop Samba for shares will require the following to be undertaken.

1. Create some MSI's for Kerberos for Windows (provided by MIT) and OpenAFS and maybe some configuration (depending on MSI flexibility) and add a GPO to install all of them onto our MDP machines
2. On user login (scriptable via MDP) run MS2MIT command which copies credentials out of the Windows cache (LSA) into the MIT cache (this is because the LSA is not accessable to other programs)
3. Add the A/D Windows users (those using our MDP machines) as trusted users in AFS (this is easy)
4. Point MyDocuments at the users home directory equivalent AFS volume automatically via login scripts, as well as any other shared areas currently mounted via Samba

Everything should then "just work" assuming we have a trust link with A/D (where MDP users get their credentials from). The trust link provides a connection from A/D -> EASE -> INF and we use this to obtain a local INF AFS session key from the users A/D principal.

However we do not currently have this trust link as EUCS have been reluctant to provide one. If EUCS decline to give us a trust link with A/D then the user will need to make an extra login step (the Kerberos for Windows login) before AFS will work - which also means they will have two sets of credentials on the machine which will cause some confusion.

D. Other Points

1. The interaction and usability of the staffmail service is much more acceptable because EUCS was prepared to work with us to add a trust link with their KDC and consequently make some reasonable provision for us to use that service with regard to our SSO infrastructure.
2. The EUCS attitude to service risk appears to be lower than ours.
3. MIT operate two realms for example, a UCS (central) realm and an LCS realm (Lab for CS) so that the LCS development is not restricted by the commodity requirement of the rest of the college - if they can do this (the originators of Kerberos) why can't we?

The views expressed in this document are those of the individual authors and do not necessarily reflect the views and policies of the School of Informatics.