

Kerberos & eDirectory integration

Bridget Lewis



Agenda

- Background
- Aims
- Technical Details
- Demo
- Caveats
- Futures

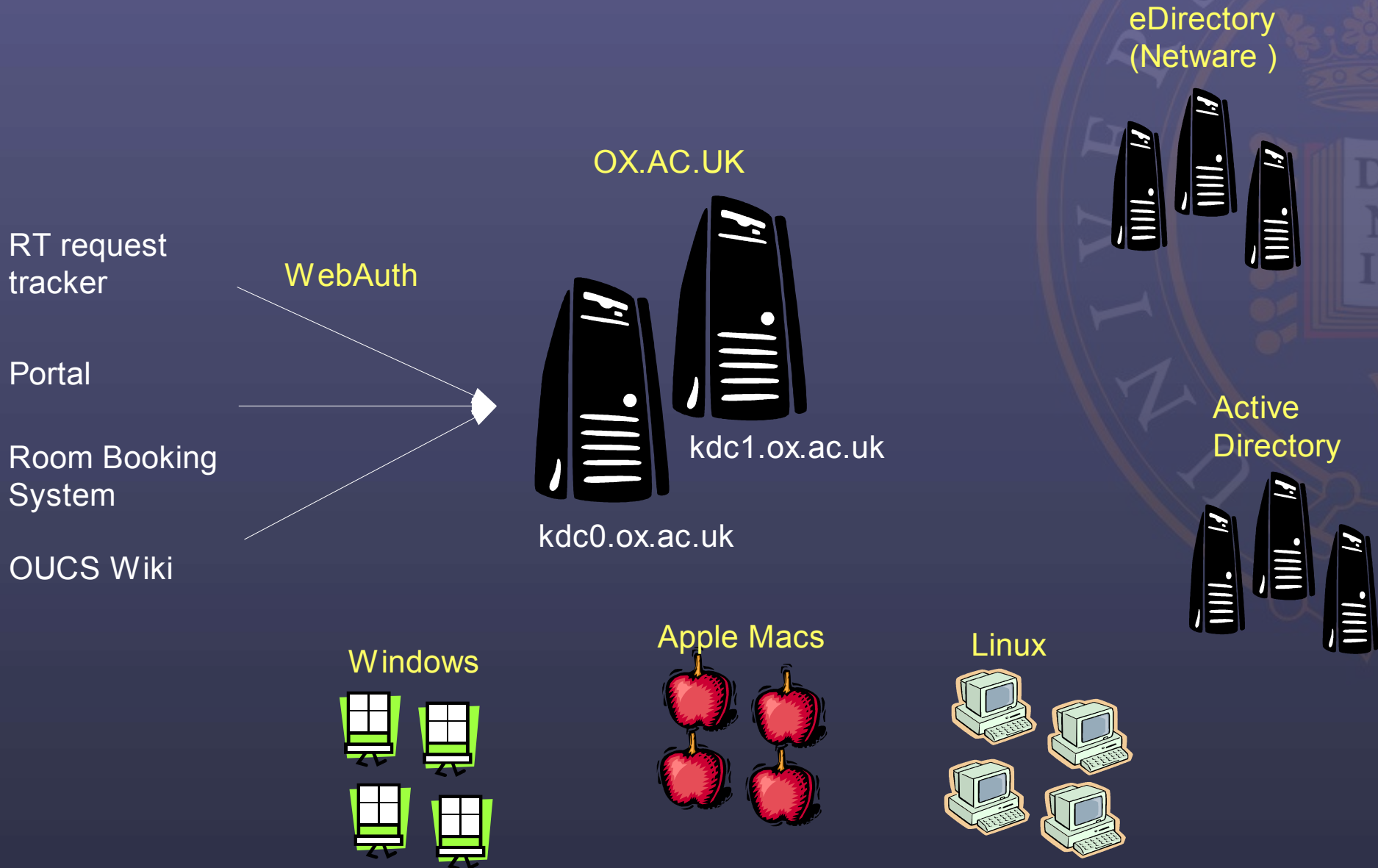


Agenda

- Background
 - Kerberos in OUCS
 - WebAuth
 - Netware in OUCS
- Aims
- Technical Considerations
- Demo
- Futures



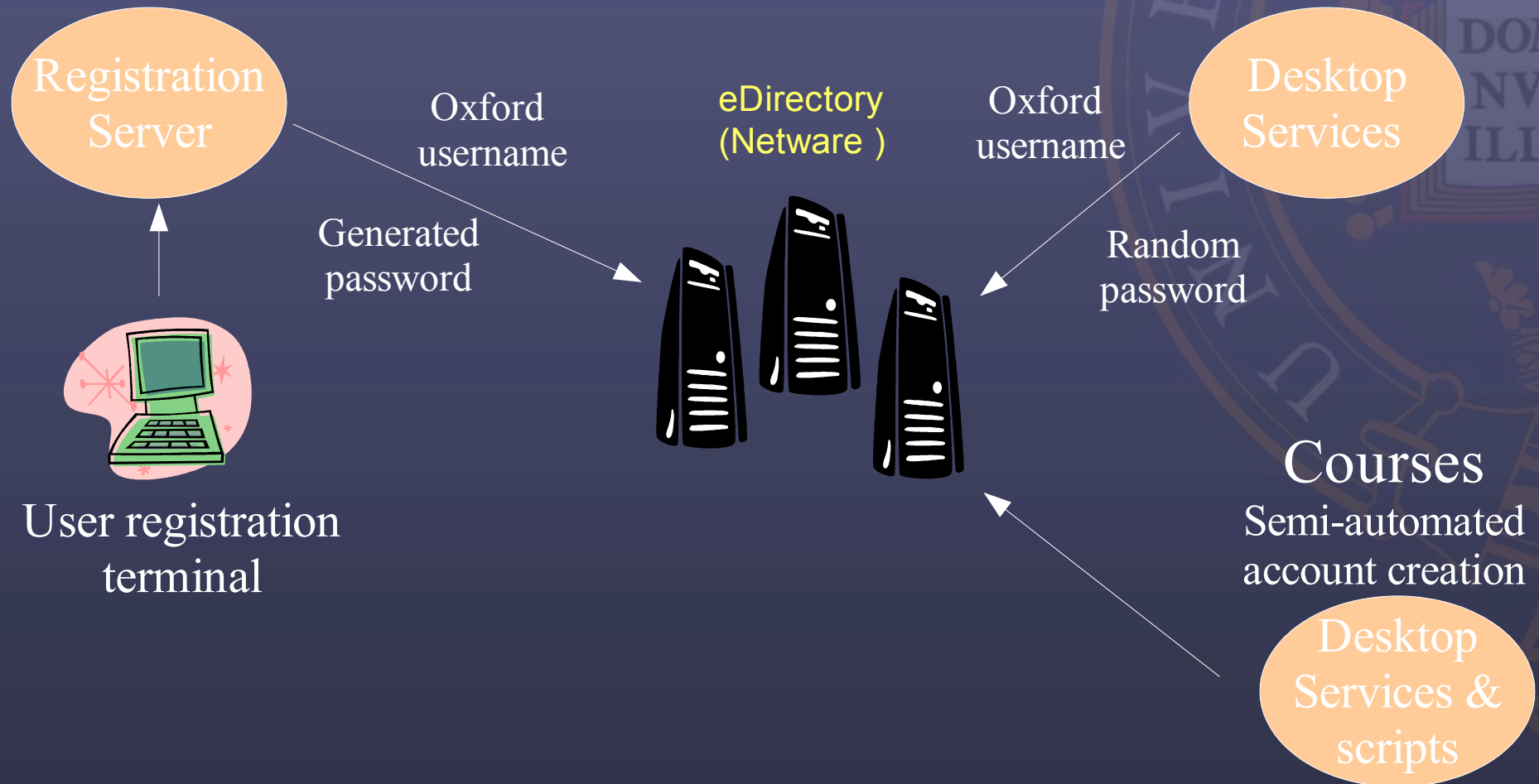
Kerberos in OUCS



Netware in OUCS

Help Centre
Automated
account creation

OUCS Staff
Manual account
creation



Agenda

- Background
- Aims
- Technical Details
- Demo
- Caveats
- Futures



Aims

- Allow users to authenticate to in-house services via Oxford username and Kerberos password
- Automatically provision eDirectory
- Investigate options which may help ITSS in departments and colleges

Agenda

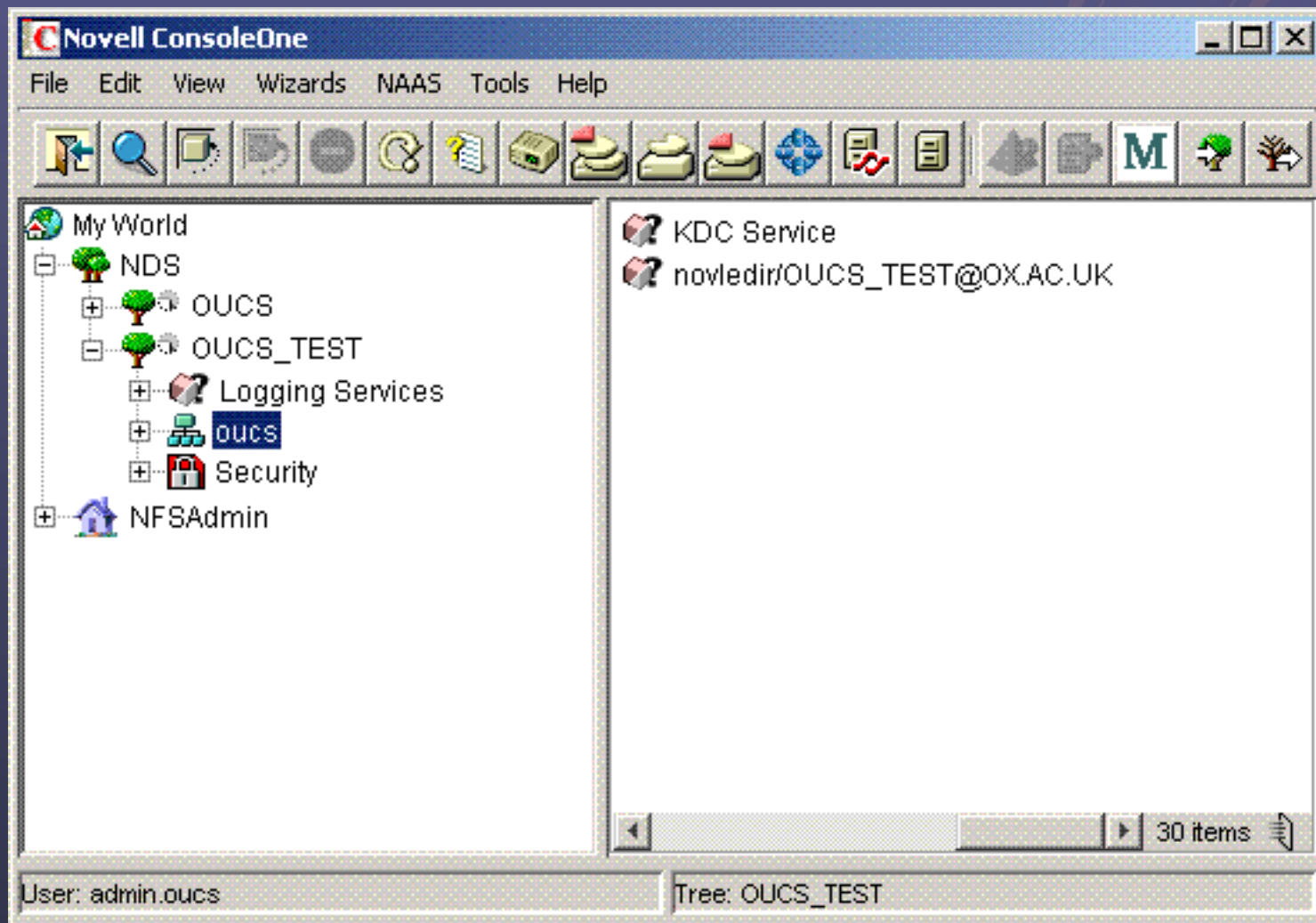
- Background
- Aims
- Technical Details
 - NMAS Kerberos Login Method
 - Installation and Configuration
 - How it works
- Demo
- Caveats
- Futures



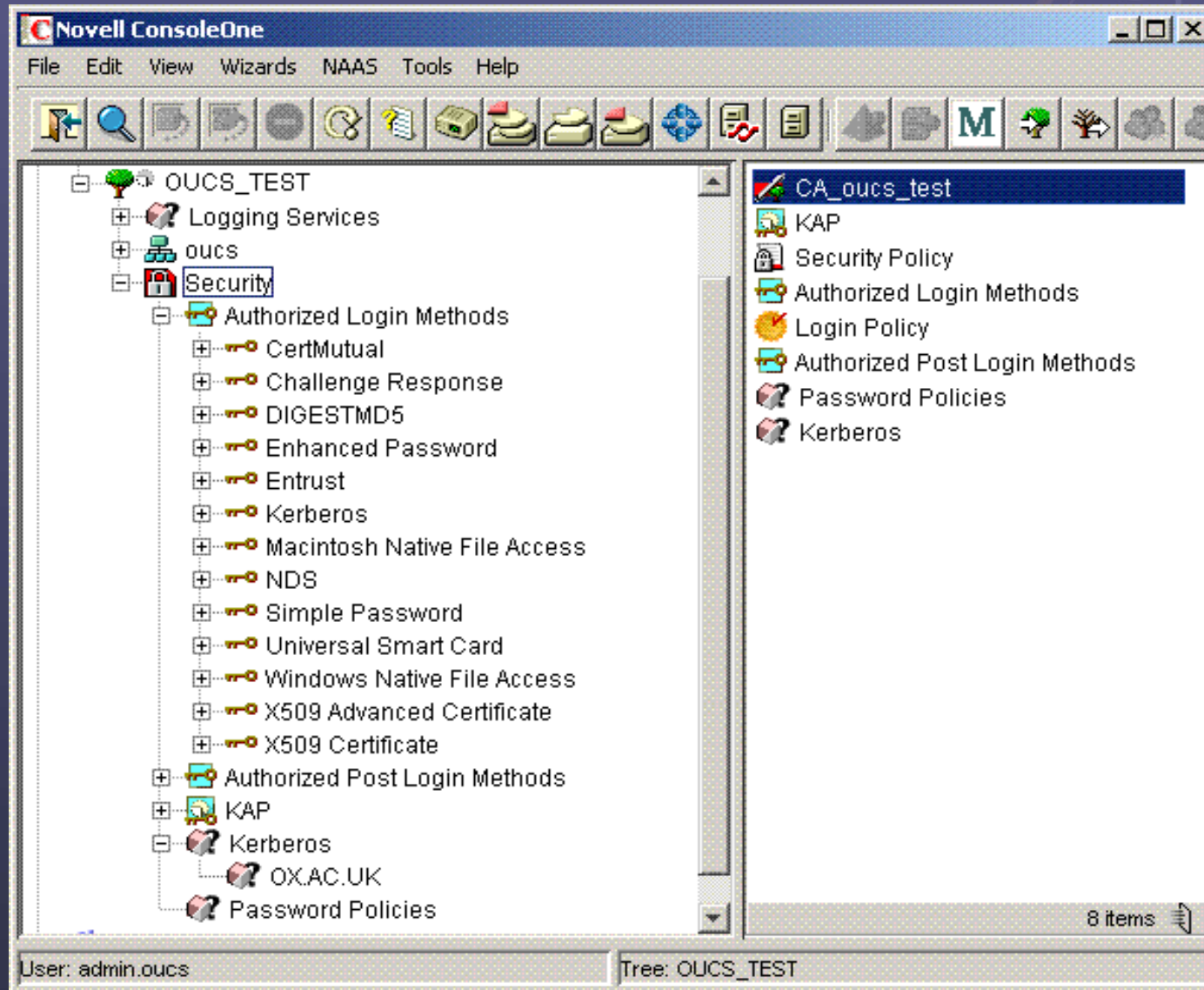
NMAS Kerberos Method?

- Novell Modular Authentication Service
 - Methods for authenticating to eDir, e.g. Smartcards, certificates
- Additional method from Novell, allowing authentication to eDir using Kerberos tickets
- Works with various Kerberos v5 KDCs
- Requires NMAS Server v2.2.0 or above
- Requires Windows 98SE, NT4, 2000 or XP
- Requires Client 4.83 or above with NMAS

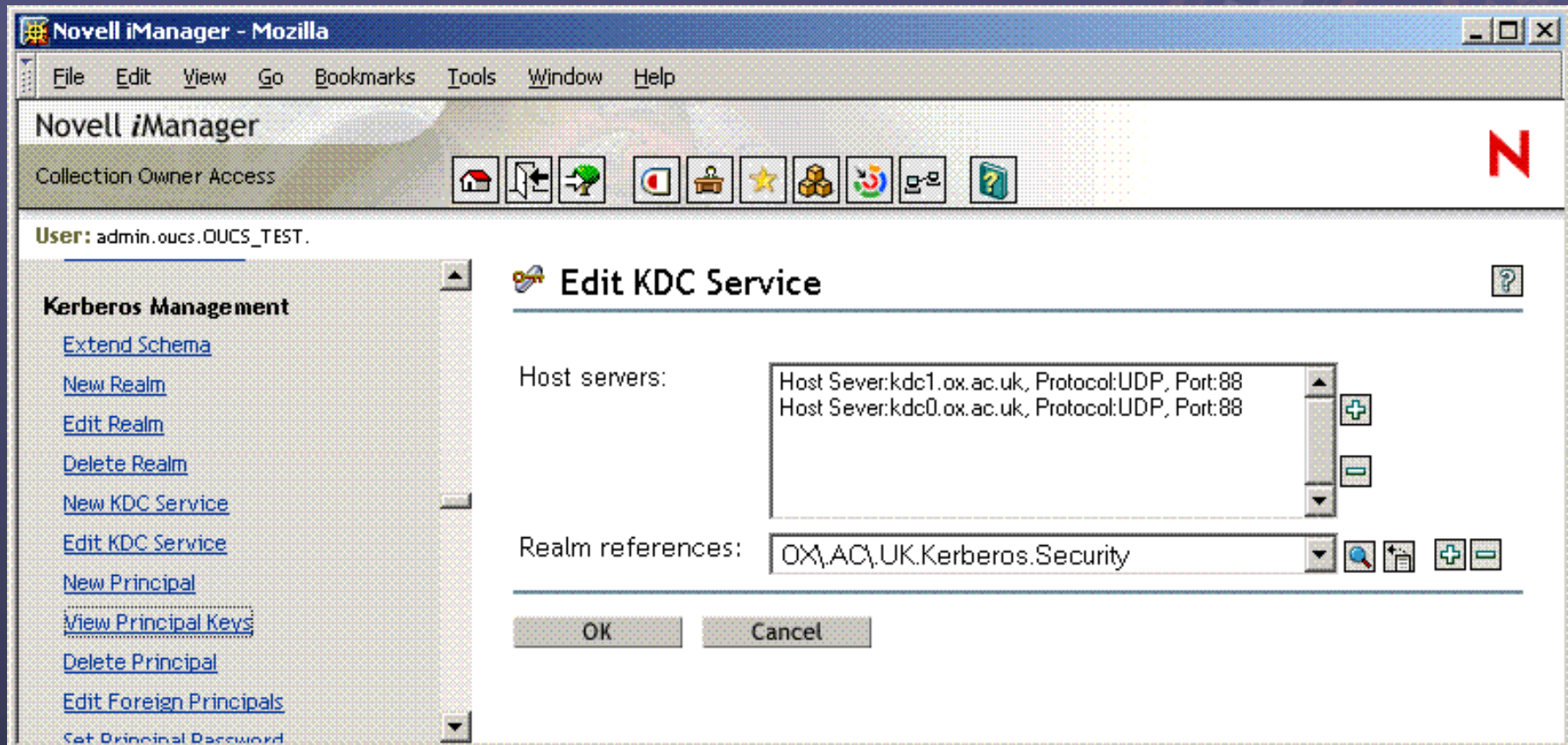
Installation and Configuration



Installation and Configuration



Installation and Configuration



Installation and Configuration

The screenshot shows a Mozilla browser window titled "Novell iManager - Mozilla". The address bar contains "Novell iManager" and the page content is for "Collection Owner Access". The user is logged in as "admin.oucs.OUCS_TEST".

The main content area displays the "Edit Realm" configuration dialog. The "Encryption type" section is expanded, showing two columns: "Supported" and "Default".

Supported:	Default:
<input checked="" type="checkbox"/> DES-CBC-CRC	<input checked="" type="radio"/> DES-CBC-CRC
<input checked="" type="checkbox"/> DES-CBC-MD5	<input type="radio"/> DES-CBC-MD5
<input checked="" type="checkbox"/> DES3-CBC-MD5	<input type="radio"/> DES3-CBC-MD5

Below the encryption type section, the "Realm sub tree" is set to "oucs". The "Sub tree search scope" is set to "Subtree" (Selected). The "KDC Services" are set to "KDC Service.oucs".

At the bottom of the dialog are "OK" and "Cancel" buttons.

Installation and Configuration

The screenshot shows a Mozilla browser window titled "Novell iManager - Mozilla". The address bar displays "Novell iManager" and "Collection Owner Access". The user is logged in as "admin.oucs.OUCS_TEST.". The left sidebar contains a "Kerberos Management" menu with options: Extend Schema, New Realm, Edit Realm, Delete Realm, New KDC Service, Edit KDC Service, New Principal, View Principal Keys, Delete Principal, Edit Foreign Principals, and Set Principal Password. Below this is an "LDAP" section with "Create LDAP Object" and "Delete LDAP Object". The main content area is titled "Edit Foreign Principals" and includes a red asterisk note "*=required". The text "Add or remove foreign principal names." is followed by an empty input field with plus and minus icons. Below that, a list box labeled "Foreign Principal Names:" contains the entry "abcd0123@OX.AC.UK". At the bottom are "OK" and "Cancel" buttons.

How it Works

- User provides username and context information
- NMAS client queries eDirectory for Kerberos principal name and realm
- NMAS client authenticates using KDC acquiring TGT and eDir service ticket
- NMAS client presents service ticket to eDir
- NMAS server grants access to eDir services

Extras

- Novl2mit utility will populate MIT Kerberos client credential cache
- Unlocking a locked workstation obtains new a TGT and service ticket from the KDC

Agenda

- Background
- Aims
- Technical Details
- Demo
- Caveats
- Futures



Demo



Agenda

- Background
- Aims
- Technical Details
- Demo
- **Caveats**
- Futures



Caveats

- Only possible for services that use Client 32
- Have not investigated authenticating to eDir and AD on the same workstation
- Tickets obtained are not renewable by default

Agenda

- Background
- Aims
- Technical Details
- Demo
- Caveats
- Futures
 - OUCS
 - Elsewhere



Kerberos in the Help Centre

Help Centre
Automated
account creation



User registration
terminal

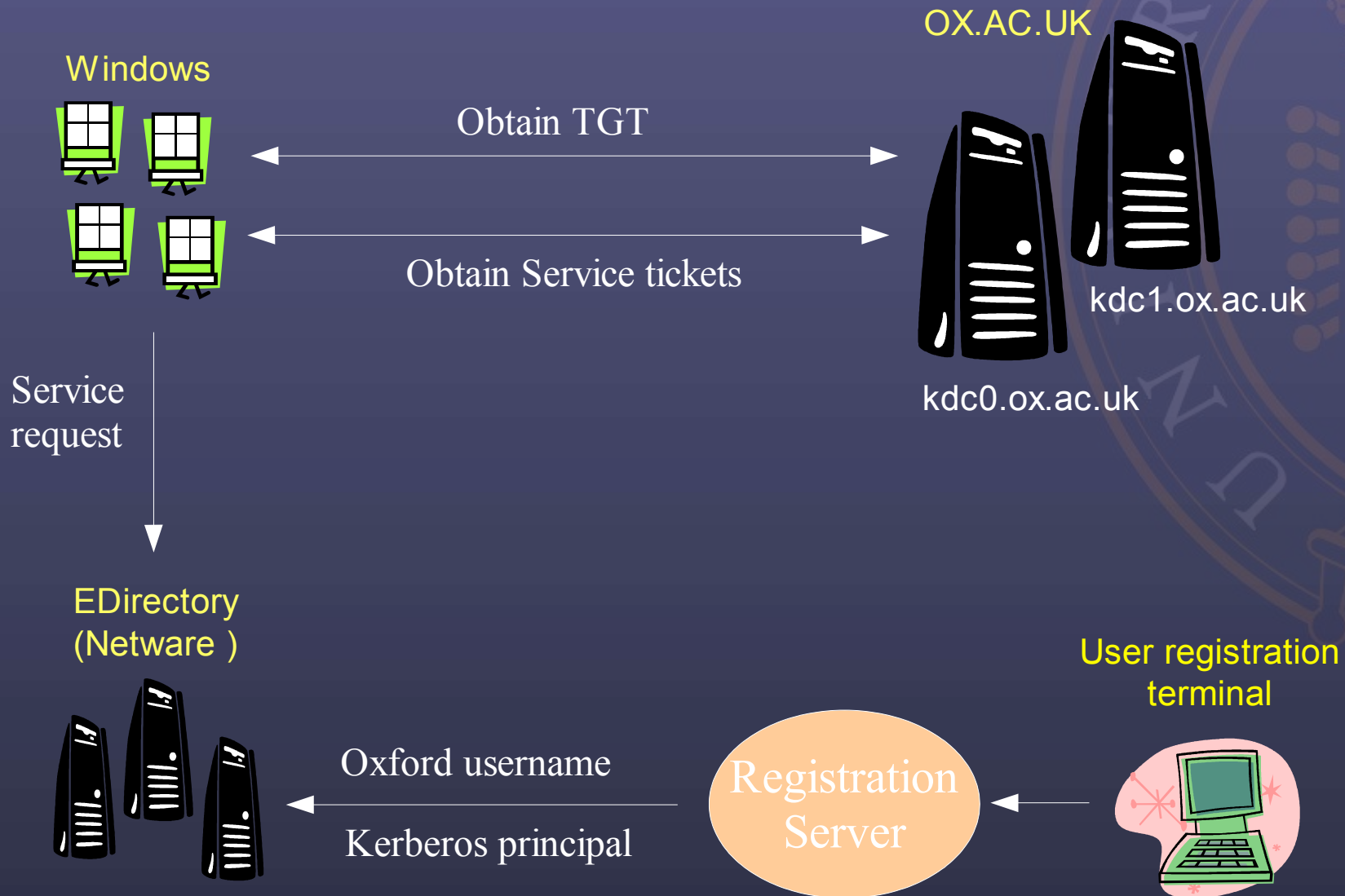
“Oxford”
username

Generated
password

EDirectory
(Netware)



Kerberos in the Help Centre



Kerberos in Departments and Colleges

- Depends on individual circumstances
- Compromises may be required (Client32 limitation)
 - Either by providing more limited services,
 - Or by users maintaining two or more username/password combinations

Questions?



References

- Download from Novell (search for Kerberos)
 - <http://download.novell.com/>
- Novell Documentation
 - <http://www.novell.com/documentation/nmaslm/treetitl.html>
- OUCS Resources
 - <http://www.oucs.ox.ac.uk/webauth/>
 - <http://users.ox.ac.uk/~pod/talks/itssc-webauth-krb5-2004-06-24/>
 - <http://users.ox.ac.uk/~raym/talks/tssso.2004-01-26/>
- General Kerberos Guides
 - <http://www.isi.edu/~brian/security/kerberos.html>
 - <http://web.mit.edu/kerberos/www/>
- University of Michigan
 - <http://www.umich.edu/~lannos/novell/kerberos.html>