

Active Directory and Oxford Single Sign-On

Bridget Lewis – ICTST Adrian Parks – OUCS

21st June 2007

Aim

 How to link Active Directory to the Oxford Kerberos Single sign-on (SSO) infrastructure

What is Kerberos?

- Authentication protocol
 Not authorisation
- Client and server mutually authenticate

Authentication vs Authorisation









Authenticated

Guest List

Donald Duck Fred Smith Lucy Jones The Doctor Fred A. Stair

Authorized

Why Kerberos?

- Single sign-on
- Centralised authentication
- Strong encryption
- No passwords over the wire

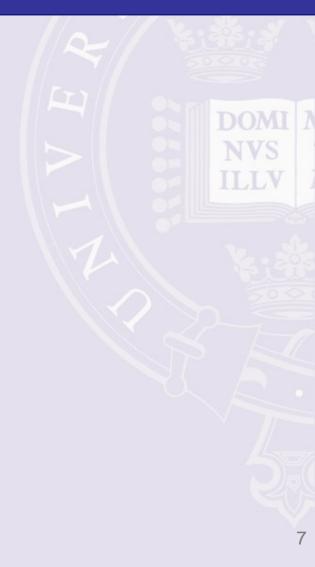


Kerberos in Oxford

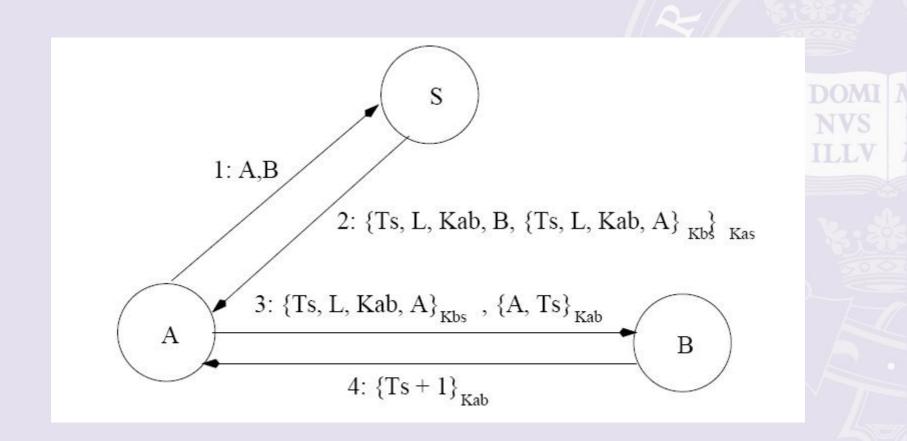
- Herald
- WebLearn
- Apache/IIS webservers (via Webauth)
- eDirectory
- Active Directory
- Open Directory

So how does it work...?

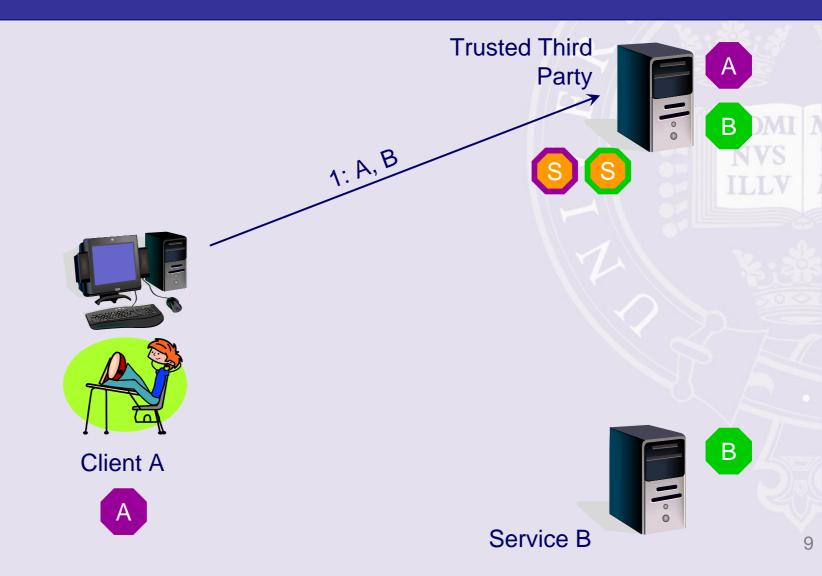
Simple, really...



Like this...



Basic Kerberos Functionality



Essential Terminology

- Principal user or service with credentials
- Ticket issued for access to a service
- Key Distribution Centre (KDC) issues tickets for principals in a realm
- Realm set of principals in a Kerberos database, e.g. OX.AC.UK, OUCS.OX.AC.UK
- TGT (ticket-granting ticket) confirms identity; used to obtain further tickets (Single Sign-on)

Kerberos and Active Directory

- Kerberos 5 implemented in AD (with added...)
 - Every domain is a Kerberos Realm
 - Every domain controller is a KDC
- Many services can use Kerberos

 CIFS, LDAP, HTTP
- Kerberos is preferred over NTLM
- Trusts between Kerberos Realms

Integrating Active Directory with Oxford Kerberos Realm

 Configure Active Directory Kerberos realm to trust Oxford Kerberos realm for authentication

2

3

Client A

KDCs

KDCs

OUCS.OX.AC.UK

Trust

Active Directory

Integrating Active Directory with Oxford Kerberos Realm

- Authorization: AD uses SID, not username to determine what a user can do
 - Usernames must exist in AD (Identity Management)
 - Oxford usernames must be mapped to Active Directory users



fred@OX.AC.UK



fred@OUCS.OX.AC.UK

So what does this mean in practice?

The "Good"...

- Use Oxford account to authenticate to AD
- No need to issue passwords to new students each year
- Devolve password problems to OUCS

Case Study

- St Hugh's College
 - ~ 20 Public Access PCs
 - -~ 600 Students, intake of ~120 per year

- Passwords were issued manually each year

- Integrated with Oxford KDCs
 - Account creation simplified via VB script
 - Students use "Herald" password
 - Administrative overhead reduced for ITSS

Case Study

- Language Centre
 - User base is whole university!
 - Potentially 40000 users
 - Historically, all used one shared account
- Webauth plus Oxford SSO solution
 - Users register for AD account via Webauth protected site
 - AD account generated on the fly
 - Log in to AD via the Oxford SSO solution
 - "Herald password"

But...there are some caveats

The "Bad"...

- Access from PCs not in domain
 Including via web, e.g. Outlook WebAccess
- Some students don't know their Oxford password (approx 13%)
- Loss of external connectivity to central KDCs

...and some problems

- The "Ugly"...
- Fallback authentication is NTLM
 - KDCs don't speak NTLM
 - Some apps only speak NTLM
- Problems integrating other operating systems (OS X, other?)

Summary

- Works very well in certain scenarios

 E.g. shared filestore for students
 Reduced administrative overhead
- Not appropriate for all environments
 - E.g. many services built on Active Directory (Exchange, Sharepoint, Web access to files etc.)

Full details are on the ITSS wiki:

https://wiki.oucs.ox.ac.uk/itss/KerberosADTrust

 Check time is in sync (throughout domain and to ntp source)

See appendix for details!



2. Request a Kerberos principal from the OUCS Systems Development team (sysdev@oucs.ox.ac.uk)

krbtgt/FULL.AD.DOMAIN.NAME

krbtgt/STHUGHS.OX.AC.UK krbtgt/ZOO.OX.AC.UK

3. Change the password of the new principal (use linux.ox.ac.uk):

adrianp@crow:~\$ /usr/sbin/kadmin -p adrianp/itss Authenticating as principal adrianp/itss with password. Password for adrianp/itss@OX.AC.UK: kadmin: cpw -e "des-cbc-crc:normal" krbtgt/OUCS-TEST.OX.AC.UK Enter password for principal "krbtgt/OUCS-TEST.OX.AC.UK": Re-enter password for principal "krbtgt/OUCS-TEST.OX.AC.UK": Password for "krbtgt/OUCS-TEST.OX.AC.UK@OX.AC.UK" changed. kadmin: quit adrianp@crow:~\$

4. Check time is in sync



5. On all domain controllers, member servers and workstations, install the Windows Support Tools and run:

ksetup /addkdc OX. AC. UK kdcO. ox. ac. uk ksetup /addkdc OX. AC. UK kdc1. ox. ac. uk ksetup /addkdc OX. AC. UK kdc2. ox. ac. uk

Or use a registry file/Group Policy (see wiki)

C:\WINDOWS\system32\cmd.exe

```
Microsoft Windows [Version 5.2.3790]
(C) Copyright 1985-2003 Microsoft Corp.
```

C:\Documents and Settings\administrator.STHUGHS>ksetup default realm = sthughs.ox.ac.uk (NT Domain) OX.AC.UK:

```
kdc = kdc0.ox.ac.uk
kdc = kdc1.ox.ac.uk
kdc = kdc2.ox.ac.uk
Realm Flags = 0x0 none
No user mappings defined.
```

C:\Documents and Settings\administrator.STHUGHS>_

_

 Create a one-way, outgoing, transitive trust between the Kerberos realm OX.AC.UK and the Active Directory forest

Use the password set in step 3.

Domain Name OX.AC.UK	Trust Type Realm	Transitive Yes	<u>Properties</u> <u>R</u> emove		DO/ NV ILL
				1	
D <u>o</u> mains that trust this Domain Name		ts): Transitive	Properties Remo <u>v</u> e		

7. Check time is in sync



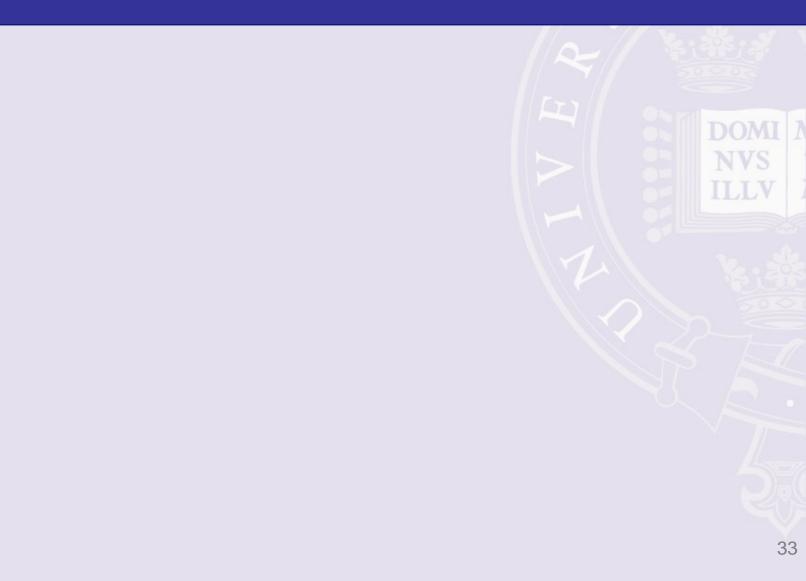
- 8. Add a name mapping for AD account to the Kerberos realm
- Format is oucs1234@OX.AC.UK
- Note uppercase OX.AC.UK



9. Reboot workstation and log in

Log On to Wi	indows	
	Windows Server 2003 R2 Standard Edition	
Copyright © 2005	Microsoft Corporation Microsoft	
User name:		St I
Password:		
Log on to:	OX.AC.UK (Kerberos Realm) OX.AC.UK (Kerberos Realm) STHUGHS Options <<	

Demo



Contact details

bridget.lewis@ict.ox.ac.uk

adrian.parks@oucs.ox.ac.uk

Some links

ITSS Wiki: https://wiki.oucs.ox.ac.uk/itss/KerberosADTrust

MIT: Designing an Authentication System: A Dialogue in Four Scenes <u>http://web.mit.edu/kerberos/www/dialogue.html</u>

Microsoft: http://www.microsoft.com/technet/prodtechnol/windows2000serv/howto/kerbstep.mspx

Kerberos: The Definitive Guide (Jason Garman/O'Reilly) http://www.amazon.co.uk/Kerberos-Definitive-Guide-Jason-Garman/dp/0596004036/ref=sr_1_1/202-9173258-1666237?ie=UTF8&s=books&gid=1182273864&sr=8-1

Appendix A — Utilities

- 2003 Resource Kit Utilities
 Kerbtray (GUI)
 - Klist (command line)
- Support Tools Utilities (from 2003 CD)
 - Ksetup (command line)
 - Ktpass (command line)

Kerbtray

- Kerbtray displays tickets
- Picture shows TGTs for ITSSCONFADDE MO.OX.AC.UK and OX.AC.UK

Kerberos Tickets 🛛 🗙
Client Principal abcd0123@0X.AC.UK
OXACUK krbtgt/ITSSCONFADDEM0.0X.AC.UK krbtgt/0X.AC.UK krbtgt/0X.AC.UK cifs/ITSSCONFADDEM0.0X.AC.UK cifs/ITSS-CONF-DC itssconfaddemo ox ac uk Image: Comparison of the seconfaddemo ox ac uk Image: Comparison of the seconfaddemo ox ac uk Image: Comparison of the seconfaddemo ox ac uk
Names Times Flags Encryption types
Ticket Encryption Type
Key Encryption Type
Close

Kerbtray

 Picture shows tickets for services in Active Directory Realm

Kerberos Tickets
Client Principal abcd0123@0X.AC.UK
ITSSCONFADDEMO.OX.AC.UK cifs/ITSS-CONF-DC.itssconfaddemo.ox.ac.uk host/itss-conf-xpsp2.itssconfaddemo.ox.ac.uk LDAP/ITSS-CONF-DC.itssconfaddemo.ox.ac.uk Idap/ITSS-CONF-DC.itssconfaddemo.ox.ac.uk
▲ ► ► ► ► ► ► ► ► ► ► ► ► ► ► ► ► ► ► ►
Names Times Flags Encryption types
Ticket Encryption Type
Key Encryption Type

Klist

_ 🗆 🗙

• Klist — as Kerbtray but command line

C:\WINDOWS\system32\cmd.exe

C:\Documents and Settings\abcd0123.ITSSCONFADDEMO\My Documents>klist Ticket cache: MSLSA: Default principal: abcd012300X.AC.UK Valid starting Expires Service principal 06/19/07 18:44:23 06/20/07 04:30:55 krbtgt/OX.AC.UKCOX.AC.UK renew until 06/26/07 18:30:55 06/19/07 18:30:55 krbtgt/ITSSCONFADDEMO.OX.AC.UK@OX.AC.UK 06/20/07 04:30:55 renew until 06/26/07 18:30:55 06/19/07 18:30:55 06/20/07 04:30:55 krbtgt/OX.AC.UK@OX.AC.UK renew until 06/26/07 18:30:55 06/19/07 18:30:58 06/20/07 04:30:55 cifs/ITSS-CONF-DC.itssconfaddemo.ox.ac.uk@ ITSSCONFADDEMO.OX.AC.UK renew until 06/26/07 18:30:55 06/19/07 18:30:58 ldap/ITSS-CONF-DC.itssconfaddemo.ox.ac.uk/ 06/20/07 04:30:55 itssconfaddemo.ox.ac.uk@ITSSCONFADDEMO.OX.AC.UK renew until 06/26/07 18:30:55 06/20/07 04:30:55 LDAP/ITSS-CONF-DC.itssconfaddemo.ox.ac.uk@ 06/19/07 18:30:55 ITSSCONFADDEMO.OX.AC.UK renew until 06/26/07 18:30:55 06/19/07 18:30:55 06/20/07 04:30:55 host/itss-conf-xpsp2.itssconfaddemo.ox.ac. uk@ITSSCONFADDEMO.OX.AC.UK renew until 06/26/07 18:30:55 C:\Documents and Settings\abcd0123.ITSSCONFADDEM0\My Documents>_

Support Tools

- Ksetup
 - Set up realm information
 - E.g. set KDCs for a given realm
- Ktpass
 - Manipulating principals

MIT Kerberos for Windows

- <u>http://web.mit.edu/kerberos/dist/</u>
- Another way of viewing tickets
- Maintains its own ticket cache
- Can import tickets from Microsoft cache
- Some applications can use these tickets

Network Identity Manager

Network Identity Manager File Gredential View Options Help File Gredential Service Name Time Remaining File Gredentials File File File Gredentials File API:abcd0123@0X.AC.UK (Default) Pile File API:abcd0123@0X.AC.UK 9 hours 55 minutes Pile API:abcd0123@0X.AC.UK 9 hours 55 minutes Pile Pile API:abcd0123@0X.AC.UK 9 hours 55 minutes Pile Pile API:abcd0123@0X.AC.UK 9 hours 55 minutes Pile Pile Arbity/OX.AC.UK@0X.AC.UK 9 hours 55 minutes Pile Pile Arbity/OX.AC.UK@0X.AC.UK Seconfaddemo.ox.ac.uk@ITSSCONFADDEMO.0X.AC.UK Pile Pile Host/itss-conf-xpsp2.itssconfaddemo.ox.ac.uk@ITSSCONFADDEMO.0X.AC.UK 9 hours 55 minutes Pile MisLSA: Krbtgt/OX.AC.UK@0X.AC.UK Pile									
Image: Service Name Time Remaining Image: Service Name Service Name Service Name Image: Service	🔊 Network Identity Man	ager	- 🗆 ×						
Image: Control of the system of the syste	<u>File</u> <u>Credential</u> <u>View</u> <u>Option</u>	is <u>H</u> elp							
Image: Control of the system of the syste	1 1 1 1	* 💿 🚺							
Kerberos v5 credentials API:abcd0123@0X.AC.UK krbtgt/0X.AC.UK@0X.AC.UK y hours 55 minutes iii LDAP/ITSS-CONF-DC.itssconfaddemo.ox.ac.uk@ITSSCONFADDEM0.0X.AC.UK y hours 55 minutes iiii cifs/ITSS-CONF-DC.itssconfaddemo.ox.ac.uk@ITSSCONFADDEM0.0X.AC.UK y hours 55 minutes iiiiii iiiiiiiiiiiiiiiiiiiiiiiiiiiiiiiiiiii	7 Identity Type Location	Service Name	Time Remaining 🔺						
Interview in detected Image: APPLabed0123@0X.AC.UK Image: APPLabed013W.AC.UK@0X.AC.UK	🗆 🕀 🚺 abcd0123@	OX.AC.UK (Default)							
Image: Strict Construction 9 hours 55 minutes Image: Strict Construct C	🛛 Kerberos v5 c	redentials							
LDAP/ITSS-CONF-DC.itssconfaddemo.ox.ac.uk@ITSSCONFADDEM0.0X.AC.UK 9 hours 55 minutes iiiiiiiiiiiiiiiiiiiiiiiiiiiiiiiiiiii	API:	abod0123@0X.AC.UK							
cifs/ITSS-CONF-DC.itssconfaddemo.ox.ac.uk@ITSSCONFADDEM0.0X.AC.UK 9 hours 55 minutes host/itss-conf-xpsp2.itssconfaddemo.ox.ac.uk@ITSSCONFADDEM0.0X.AC.UK 9 hours 55 minutes krbtgt/ITSSCONFADDEM0.0X.AC.UK@0X.AC.UK 9 hours 55 minutes Idap/ITSS-CONF-DC.itssconfaddemo.ox.ac.uk/itssconfaddemo.ox.ac.uk@ITSSCONFADDEM0.0X.AC.UK 9 hours 55 minutes MSLSA: krbtgt/0X.AC.UK@0X.AC.UK 9 hours 55 minutes krbtgt/0X.AC.UK@0X.AC.UK 9 hours 55 minutes 9 hours 55 minutes krbtgt/0X.AC.UK@0X.AC.UK 9 hours 55 minutes 9 hours 55 minutes is krbtgt/0X.AC.UK@0X.AC.UK 9 hours 55 minutes is krbtgt/ITSS-CONF-DC.itssconfaddemo.ox.ac.uk@ITSSCONFADDEM0.0X.AC.UK 9 hours 55 minutes is cifs/ITSS-CONF-DC.itssconfaddemo.ox.ac.uk@ITSSCONFADDEM0.0X.AC.UK 9 hours 55 minutes is host/itss-conf-xpsp2.itssconfaddemo.ox.ac.uk@ITSSCONFADDEM0.0X.AC.UK 9 hours 55 minutes		krbtgt/0X.AC.UK@0X.AC.UK	9 hours 55 minutes						
Idap/ITSS-CONF-DC.itssconfaddemo.ox.ac.uk/itssconfaddemo.ox.ac.uk@ITSSCONFADDEMO.OX.AC.UK 9 hours 55 minutes MSLSA: 9 hours 55 minutes Idap/ITSS-CONF-DC.itssconfaddemo.ox.ac.uk@ITSSCONFADDEMO.OX.AC.UK 9 hours 55 minutes		LDAP/ITSS-CONF-DC.itssconfaddemo.ox.ac.uk@ITSSCONFADDEMO.0X.AC.UK	9 hours 55 minutes						
Idap/ITSS-CONF-DC.itssconfaddemo.ox.ac.uk/itssconfaddemo.ox.ac.uk@ITSSCONFADDEMO.OX.AC.UK 9 hours 55 minutes MSLSA: 9 hours 55 minutes Idap/ITSS-CONF-DC.itssconfaddemo.ox.ac.uk@ITSSCONFADDEMO.OX.AC.UK 9 hours 55 minutes		9 hours 55 minutes							
Idap/ITSS-CONF-DC.itssconfaddemo.ox.ac.uk/itssconfaddemo.ox.ac.uk@ITSSCONFADDEMO.OX.AC.UK 9 hours 55 minutes MSLSA: 9 hours 55 minutes Idap/ITSS-CONF-DC.itssconfaddemo.ox.ac.uk@ITSSCONFADDEMO.OX.AC.UK 9 hours 55 minutes	1. 1. 1. 1. 1. 1. 1. 1. 1. 1. 1. 1. 1. 1	host/itss-conf-xpsp2.itssconfaddemo.ox.ac.uk@ITSSCONFADDEM0.0X.AC.UK							
Image: MSLSA: krbtgt/0X.AC.UK@0X.AC.UK 9 hours 55 minutes Image: MSLSA: 9 hours 55 minutes		krbtgt/ITSSCONFADDEMO.0X.AC.UK@0X.AC.UK	9 hours 55 minutes						
krbtgt/0X.AC.UK@0X.AC.UK 9 hours 55 minutes LDAP/ITSS-CONF-DC.itssconfaddemo.ox.ac.uk@ITSSCONFADDEM0.0X.AC.UK 9 hours 55 minutes cifs/ITSS-CONF-DC.itssconfaddemo.ox.ac.uk@ITSSCONFADDEM0.0X.AC.UK 9 hours 55 minutes host/itss-conf-xpsp2.itssconfaddemo.ox.ac.uk@ITSSCONFADDEM0.0X.AC.UK 9 hours 55 minutes		ldap/ITSS-CONF-DC.itssconfaddemo.ox.ac.uk/itssconfaddemo.ox.ac.uk@ITSSCONFADDEMO.OX.AC.UK	9 hours 55 minutes						
LDAP/ITSS-CONF-DC.itssconfaddemo.ox.ac.uk@ITSSCONFADDEM0.0X.AC.UK 9 hours 55 minutes ifs/ITSS-CONF-DC.itssconfaddemo.ox.ac.uk@ITSSCONFADDEM0.0X.AC.UK 9 hours 55 minutes host/itss-conf-xpsp2.itssconfaddemo.ox.ac.uk@ITSSCONFADDEM0.0X.AC.UK 9 hours 55 minutes	B MSL	SA:							
cifs/ITSS-CONF-DC.itssconfaddemo.ox.ac.uk@ITSSCONFADDEM0.0X.AC.UK 9 hours 55 minutes host/itss-conf-xpsp2.itssconfaddemo.ox.ac.uk@ITSSCONFADDEM0.0X.AC.UK 9 hours 55 minutes		krbtgt/0X.AC.UK@0X.AC.UK	9 hours 55 minutes						
host/itss-conf-xpsp2.itssconfaddemo.ox.ac.uk@ITSSCONFADDEM0.0X.AC.UK 9 hours 55 minutes	2.4 2.5	9 hours 55 minutes							
host/itss-conf-xpsp2.itssconfaddemo.ox.ac.uk@ITSSCONFADDEM0.0X.AC.UK 9 hours 55 minutes		9 hours 55 minutes							
		9 hours 55 minutes							
krbtgt/ITSSCONFADDEMO.0X.AC.UK@0X.AC.UK 9 hours 55 minutes	83	9 hours 55 minutes							
👪 Idap/ITSS-CONF-DC.itssconfaddemo.ox.ac.uk/itssconfaddemo.ox.ac.uk@ITSSCONFADDEMO.OX.AC.UK 9 hours 55 minutes 🚽	83								

Appendix B — Additional Notes

- Time must be within 5 minutes of KDC time
- Logon may fail intermittently if logon allowed before network fully initialized (XP/2003)
 - Group Policy setting
 - Computer Configuration/ Administrative Templates/System/Logon
 - Enable setting "Always wait for network on computer startup or user logon"
- Terminal Services Patch
 - <u>http://support.microsoft.com/default.aspx?scid=KB;EN</u>
 <u>-US;902336</u>

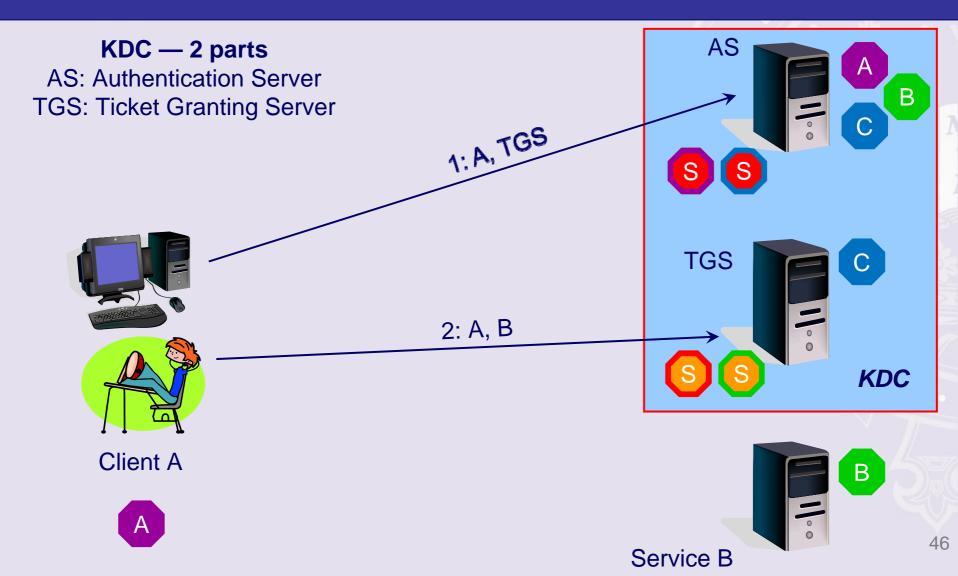
Short History of Time

- All DCs sync to PDC emulator (automatic)
- Member servers and workstations sync to Domain Controllers (automatic)
- PDC emulator must be sync'd to ntp source
 - Must update if you move PDC emulator role
 - w32tm /config /manualpeerlist: "ntpserver1 ntpserver2 ntpserver3" /syncfromflags:manual /reliable:yes /update
 - <u>http://technet2.microsoft.com/windowsserver/en/library/ce8890cf-ef46-4931-8e4a-2fc5b4ddb0471033.mspx?mfr=true</u>

Automated Account Creation

- OUCS can provide nightly update of Oxford usernames and other information to each unit
 - <u>http://www.oucs.ox.ac.uk/registration/card_dat</u>
 <u>a_2006.xml.ID=body.1_div.9</u>
 - Use scripts to feed into Active Directory

Full Kerberos Functionality



Other notes of interest

- Workstation authenticates too: problems for x-realm auth.
- DC devolution KDC patches available
- Macs
- eDir
- preauth, timestamps, lifespan of tickets etc

Appendix C

Use Wireshark to observe the Kerberos exchange

```
📶 kerb2.pcap - Wireshark
```

<u>File Edit View Go Capture Analyze Statistics Help</u>



						_
No	Time	Source	Destination	Protocol	Info	*
	2.740015	129.67.102.73	129.67.102.78	KRB5	AS-REQ	4
	2.741809	129.67.102.78	129.67.102.73	KRB5	AS-REP	
	2.746834	129.67.102.73	129.67.102.78	KRB5	TGS-REQ	
	2.748758	129.67.102.78	129.67.102.73	KRB5	TGS-REP	
	2.759838	129.67.102.73	129.67.102.78	KRB5	TGS-REQ	
	2.761270	129.67.102.78	129.67.102.73	KRB5	TGS-REP	Ξ
	2.779207	129.67.102.73	129.67.102.78	TCP	[TCP segment of a reassembled PDU]	
55	2.779478	129.67.102.73	129.67.102.78	SMB	Session Setup AndX Request	
56	2.780062	129.67.102.78	129.67.102.73	TCP	microsoft-ds > 1030 [ACK] Seq=190 Ack=2836 Win=65535 Len=0	
57	2.781212	129.67.102.78	129.67.102.73	SMB	Session Setup AndX Response	
58	2.805722	129.67.102.73	129.67.102.78	SMB	Tree Connect AndX Request, Path: \\NSMSW2K1.OUCS-TEST.OX.AC.UK\]	4
	2.806145	129.67.102.78	129.67.102.73	SMB	Tree Connect AndX Response	
	2.835381	129.67.102.73	129.67.102.78	SMB	Trans2 Request, GET_DFS_REFERRAL, File:	
	2.835898	129.67.102.78	129.67.102.73	SMB	Trans2 Response, GET_DFS_REFERRAL	
	2.994003	129.67.102.73	129.67.102.78	TCP	1030 > microsoft-ds [ACK] Seq=3036 Ack=855 Win=16666 Len=0	
63	5.757103	129.67.102.73	129.67.102.78	DNS	Standard query A kdc0.ox.ac.uk	
	5.757588	129.67.102.78	129.67.102.73	DNS	Standard querý response A 163.1.2.74	
	5.770367	129.67.102.73	163.1.2.74	KRB5	AS-REQ	
	5.774177	163.1.2.74	129.67.102.73	KRB5	KRB Error: KRB5KDC_ERR_PREAUTH_REQUIRED	
	5.836655	129.67.102.73	163.1.2.74	KRB5	AS-REQ	
68	5.840084	163.1.2.74	129.67.102.73	KRB5	AS-REP	
	5.924561	129.67.102.73	163.1.2.74	KRB5	TGS-REQ	
70	5.932478	163.1.2.74	129.67.102.73	KRB5	TGS-REP	
	5.980876	129.67.102.73	129.67.102.78	KRB5	TGS-REQ	
	5.982844	129.67.102.78	129.67.102.73	KRB5	TGS-REP	
73	7.551618	129.67.102.73	129.67.102.78	TCP	1042 > 1025 [SYN] Seq=0 Len=0 MSS=1460	
74	7.551901	129.67.102.78	129.67.102.73	TCP	1025 > 1042 [SYN, ACK] Seq=0 Ack=1 Win=16384 Len=0 MSS=1460	
	7.554437	129.67.102.73	129.67.102.78	тср	1042 > 1025 [АСК] Seq=1 Ack=1 Win=17520 Len=0	
76	7.556130	129.67.102.73	129.67.102.78	DCERPC	E Bind: call_id: 1 LSA v0.0	
	7.556607	129.67.102.78	129.67.102.73		Bind_ack: call_id: 1 accept max_xmit: 5840 max_recv: 5840	
	7.557241	129.67.102.73	129.67.102.78	LSA	LsarLookupNames4 request	Ŧ
						4

□ Type: PA-PAC-REQUEST (128)

Value: 3005A0030101FF

PAC Request: 1

⊟ KDC_REQ_BODY

Padding: 0

E Client Name (Principal): nsmsvmxp\$

Realm: OUCS-TEST.OX.AC.UK

□ Server Name (Service and Instance): krbtgt/OUCS-TEST.OX.AC.UK

Name-type: Service and Instance (2)

Name: krbtgt

Ξ

.

```
📶 kerb2.pcap - Wireshark
                                                                                                                        File Edit View Go Capture Analyze Statistics Help
       Time
                                    Destination
                                                       Protocol Info
No. -
                    Source
    48 2.740015
                                    129.67.102.78
                                                        KRB5
                                                               AS-REQ
                   129.67.102.73
    49 2.741809
                   129.67.102.78
                                    129.67.102.73
                                                        KRB5
                                                               AS-REP
    50 2.746834
                   129.67.102.73
                                    129.67.102.78
                                                        KRB5
                                                               TGS-REQ
    51 2.748758
                   129.67.102.78
                                    129.67.102.73
                                                        KRB5
                                                               TGS-REP
    52 2.759838
                   129.67.102.73
                                    129.67.102.78
                                                        KRB5
                                                               TGS-REQ
    53 2.761270
                   129.67.102.78
                                    129.67.102.73
                                                        KRB5
                                                               TGS-REP
    54 2.779207
                                   129.67.102.78
                                                               [TCP segment of a reassembled PDU]
                   129.67.102.73
                                                        TCP
    55 2.779478
                   129.67.102.73
                                    129.67.102.78
                                                        SMB
                                                               Session Setup AndX Request
                                                               microsoft-ds > 1030 [ACK] Seg=190 Ack=2836 Win=65535 Len=0
    56 2.780062
                   129.67.102.78
                                    129.67.102.73
                                                        TCP
    57 2.781212
                                                               Session Setup AndX Response
                   129.67.102.78
                                    129.67.102.73
                                                        SMB
    58 2.805722
                   129.67.102.73
                                                               Tree Connect AndX Request, Path: \\NSMSW2K1.OUCS-TEST.OX.AC.UK\]
                                    129.67.102.78
                                                        SMB
    59 2.806145
                   129.67.102.78
                                                               Tree Connect AndX Response
                                    129.67.102.73
                                                        SMB
    60 2.835381
                   129.67.102.73
                                                               Trans2 Request, GET_DFS_REFERRAL, File:
                                    129.67.102.78
                                                        SMB
    61 2.835898
                                                               Trans2 Response, GET_DFS_REFERRAL
                   129.67.102.78
                                    129.67.102.73
                                                        SMB
    62 2.994003
                   129.67.102.73
                                   129.67.102.78
                                                       TCP
                                                              1030 > microsoft-ds [ACK] Seg=3036 Ack=855 Win=16666 Len=0
                                                               Standard guery A kdc0.ox.ac.uk
    63 5.757103
                   129.67.102.73
                                    129.67.102.78
                                                        DNS
    64 5.757588
                                                               Standard query response A 163.1.2.74
                   129.67.102.78
                                    129.67.102.73
                                                        DNS
    65 5.770367
                   129.67.102.73
                                   163.1.2.74
                                                        KRB5
                                                               AS-REQ
    66 5.774177
                                                               KRB Error: KRB5KDC_ERR_PREAUTH_REQUIRED
                   163.1.2.74
                                    129.67.102.73
                                                        KRB5
    67 5.836655
                   129.67.102.73
                                    163.1.2.74
                                                        KRB5
                                                               AS-REQ
    68 5.840084
                                    129.67.102.73
                   163.1.2.74
                                                        KRB5
                                                               AS-REP
    69 5.924561
                   129.67.102.73
                                                        KRB5
                                    163.1.2.74
                                                               TGS-REQ
                                    129.67.102.73
    70 5.932478
                   163.1.2.74
                                                        KRB5
                                                               TGS-REP
    71 5.980876
                   129.67.102.73
                                   129.67.102.78
                                                        KRB5
                                                               TGS-REQ
    72 5.982844
                   129.67.102.78
                                    129.67.102.73
                                                        KRB5
                                                               TGS-REP
                                                              1042 > 1025 [SYN] Seg=0 Len=0 MSS=1460
    73 7.551618
                   129.67.102.73
                                    129.67.102.78
                                                        TCP
    74 7.551901
                                                              1025 > 1042 [SYN, ACK] Seq=0 Ack=1 Win=16384 Len=0 MSS=1460
                   129.67.102.78
                                   129.67.102.73
                                                        TCP
    75 7.554437
                                                              1042 > 1025 [ACK] Seg=1 Ack=1 Win=17520 Len=0
                   129.67.102.73
                                   129.67.102.78
                                                       TCP
    76 7.556130
                   129.67.102.73
                                   129.67.102.78
                                                        DCERPC Bind: call_id: 1 LSA V0.0
                                                        DCERPC Bind_ack: call_id: 1 accept max_xmit: 5840 max_recv: 5840
    77 7.556607
                   129.67.102.78
                                    129.67.102.73
    78 7.557241
                                                               LsarLookupNames4 request
                   129.67.102.73
                                    129.67.102.78
                                                        LSA
```

Kerberos AS-REQ

Pvno: 5 MSG Type: AS-REQ (10) ■ KDC_REQ_BODY Padding: 0 ■ KDCOptions: 40800010 (Forwardable, Renewable, Renewable OK) ■ Client Name (Principal): adrianp Realm: OX.AC.UK ■ Server Name (Service and Instance): krbtgt/OX.AC.UK Name-type: Service and Instance (2) Name: krbtgt

Manual AND AND AND

Ŧ

Ξ

н

🚺 kerb2.pcap - Wireshark	- Wireshark
--------------------------	-------------

File Edit View Go Capture Analyze Statistics Help

-	-		=1 = 7 =	- 1			
No		Time	Source	Destination	Protocol	Info	^
	48	2.740015	129.67.102.73	129.67.102.78	KRB5	AS-REQ	1
	49	2.741809	129.67.102.78	129.67.102.73	KRB5	AS-REP	
		2.746834	129.67.102.73	129.67.102.78	KRB5	TGS-REQ	
		2.748758	129.67.102.78	129.67.102.73	KRB5	TGS-REP	
		2.759838	129.67.102.73	129.67.102.78	KRB5	TGS-REQ	
		2.761270	129.67.102.78	129.67.102.73	KRB5	TGS-REP	Ε
		2.779207	129.67.102.73	129.67.102.78	TCP	[TCP segment of a reassembled PDU]	
		2.779478	129.67.102.73	129.67.102.78	SMB	Session Setup AndX Request	
		2.780062	129.67.102.78	129.67.102.73	TCP	microsoft-ds > 1030 [ACK] Seq=190 Ack=2836 Win=65535 Len=0	
		2.781212	129.67.102.78	129.67.102.73	SMB	Session Setup AndX Response	
		2.805722	129.67.102.73	129.67.102.78	SMB	Tree Connect AndX Request, Path: \\N5MSW2K1.OUC5-TEST.OX.AC.UK\]	
		2.806145	129.67.102.78	129.67.102.73	SMB	Tree Connect AndX Response	
		2.835381	129.67.102.73	129.67.102.78	SMB	Trans2 Request, GET_DFS_REFERRAL, File:	
	61	2.835898	129.67.102.78	129.67.102.73	SMB	Trans2 Response, GET_DFS_REFERRAL	
	62	2.994003	129.67.102.73	129.67.102.78	TCP	1030 > microsoft-ds [ACK] Seq=3036 Ack=855 Win=16666 Len=0	
		5.757103	129.67.102.73	129.67.102.78	DNS	Standard query A kdc0.ox.ac.uk	
		5.757588	129.67.102.78	129.67.102.73	DNS	Standard query response A 163.1.2.74	
		5.770367	129.67.102.73	163.1.2.74	KRB5	AS-REQ	
		5.774177	163.1.2.74	129.67.102.73	KRB5	KRB Error: KRB5KDC_ERR_PREAUTH_REQUIRED	
		5.836655	129.67.102.73	163.1.2.74	KRB5	A5-REQ	
	68	5.840084	163.1.2.74	129.67.102.73	KRB5	AS-REP	
		5.924561	129.67.102.73	163.1.2.74	KRB5	TGS-REQ	
	70	5.932478	163.1.2.74	129.67.102.73	KRB5	TGS-REP	
		5.980876	129.67.102.73	129.67.102.78	KRB5	TGS-REQ	
	72	5.982844	129.67.102.78	129.67.102.73	KRB5	TGS-REP	
	73	7.551618	129.67.102.73	129.67.102.78	TCP	1042 > 1025 [SYN] Seq=0 Len=0 MSS=1460	
		7.551901	129.67.102.78	129.67.102.73	TCP	1025 > 1042 [SYN, ACK] Seq=0 Ack=1 Win=16384 Len=0 MSS=1460	
	75	7.554437	129.67.102.73	129.67.102.78	TCP	1042 > 1025 [ACK] Seq=1 Ack=1 Win=17520 Len=0	
		7.556130	129.67.102.73	129.67.102.78		Bind: call_id: 1 LSA VO.0	
		7.556607	129.67.102.78	129.67.102.73	DCERPC	Bind_ack: call_id: 1 accept max_xmit: 5840 max_recv: 5840	
	78	7.557241	129.67.102.73	129.67.102.78	LSA	LsarLookupNames4 request	Ŧ
							_

Kerberos AS-REQ

Pvno: 5

MSG Type: AS-REQ (10)

padata: PA-ENC-TIMESTAMP

```
□ Type: PA-ENC-TIMESTAMP (2)
```

□ Value: 3039A003020101A10602047C9105C8A22A0428AD3905851B... des-cbc-crc

Encryption type: des-cbc-crc (1)

Kvno: 2089878984

enc PA_ENC_TIMESTAMP: AD3905851BB4BE9AB42EB167DF3D21775EF377D5A98564A7...

KDC_REQ_BODY

Padding: 0

Ξ

```
📶 kerb2.pcap - Wireshark
<u>File Edit View Go Capture Analyze Statistics Help</u>
```



۰

Ξ

÷

.

No	Time	Source	Destination	Protocol	Info	*
48	2.740015	129.67.102.73	129.67.102.78	KRB5	AS-REQ	
	2.741809	129.67.102.78	129.67.102.73	KRB5	AS-REP	
50	2.746834	129.67.102.73	129.67.102.78	KRB5	TGS-REQ	
51	2.748758	129.67.102.78	129.67.102.73	KRB5	TGS-REP	
52	2.759838	129.67.102.73	129.67.102.78	KRB5	TGS-REQ	
	2.761270	129.67.102.78	129.67.102.73	KRB5	TGS-REP	Ξ
	2.779207	129.67.102.73	129.67.102.78	TCP	[TCP segment of a reassembled PDU]	
	2.779478	129.67.102.73	129.67.102.78	SMB	Session Setup AndX Request	
	2.780062	129.67.102.78	129.67.102.73	TCP	microsoft-ds > 1030 [ACK] Seq=190 Ack=2836 Win=65535 Len=0	
	2.781212	129.67.102.78	129.67.102.73	SMB	Session Setup AndX Response	
	2.805722	129.67.102.73	129.67.102.78	SMB	Tree Connect AndX Request, Path: \\NSMSW2K1.OUCS-TEST.OX.AC.UK\]	
	2.806145	129.67.102.78	129.67.102.73	SMB	Tree Connect AndX Response	
60	2.835381	129.67.102.73	129.67.102.78	SMB	Trans2 Request, GET_DFS_REFERRAL, File:	
	2.835898	129.67.102.78	129.67.102.73	SMB	Trans2 Response, GET_DFS_REFERRAL	
	2.994003	129.67.102.73	129.67.102.78	тср	1030 > microsoft-ds [ACK] Seq=3036 Ack=855 Win=16666 Len=0	
	5.757103	129.67.102.73	129.67.102.78	DNS	Standard query A kdc0.ox.ac.uk	
	5.757588	129.67.102.78	129.67.102.73	DNS	Standard query response A 163.1.2.74	
	5.770367	129.67.102.73	163.1.2.74	KRB5	AS-REQ	
	5.774177	163.1.2.74	129.67.102.73	KRB5	KRB Error: KRB5KDC_ERR_PREAUTH_REQUIRED	
	5.836655	129.67.102.73	163.1.2.74	KRB5	AS-REQ	
	5.840084	163.1.2.74	129.67.102.73	KRB5	AS-REP	
		129.67.102.73	163.1.2.74	KRB5	TGS-REQ	
	5.932478	163.1.2.74	129.67.102.73	KRB5	TGS-REP	
	5.980876	129.67.102.73	129.67.102.78	KRB5	TGS-REQ	
	5.982844	129.67.102.78	129.67.102.73	KRB5	TGS-REP	
73	7.551618	129.67.102.73	129.67.102.78	тср	1042 > 1025 [SYN] Seq=0 Len=0 MSS=1460	
	7.551901	129.67.102.78	129.67.102.73	TCP	1025 > 1042 [SYN, ACK] Seq=0 Ack=1 Win=16384 Len=0 MSS=1460	
75	7.554437	129.67.102.73	129.67.102.78	тср	1042 > 1025 [ACK] Seq=1 Ack=1 Win=17520 Len=0	
76	7.556130	129.67.102.73	129.67.102.78		Bind: call_id: 1 LSA VO.O	
	7.556607	129.67.102.78	129.67.102.73	DCERPC	Bind_ack: call_id: 1 accept max_xmit: 5840 max_recv: 5840	
78	7.557241	129.67.102.73	129.67.102.78	LSA	LsarLookupNames4 request	Ŧ
						-

```
⊟ Kerberos TGS-REQ
```

Pvno: 5
MSG Type: TGS-REQ (12)
⊞ padata: PA-TGS-REQ
□ KDC_REQ_BODY
Padding: 0
🗄 KDCOptions: 40800000 (Forwardable, Renewable)
Realm: OX.AC.UK
till: 2037-09-13 02:48:05 (Z)

Nonce: 1865634814

. 1- 1 I . . .

```
📶 kerb2.pcap - Wireshark
```

<u>File Edit View Go Capture Analyze Statistics Help</u>

 $\overline{\mathbf{v}}$

File Edit View Go	<u>Capture</u> <u>A</u> naiyze <u>S</u> ta	tistics <u>H</u> eip			
No Time	Source	Destination	Protocol	Info	^
122 13.517072		129.67.102.78		NetrLogonSamLogonWithFlags request	
123 13.517649		129.67.102.73	RPC_NE	NetrLogonSamLogonWithFlags response	
124 13.533068		129.67.102.78	TCP	1047 > ldap [SYN] Seq=0 Len=0 MSS=1460	
125 13.533293		129.67.102.73	TCP	ldap > 1047 [SYN, ACK] Seq=0 Ack=1 Win=16384 Len=0 MSS=1460	
126 13.533757		129.67.102.78	TCP	1047 > ldap [ACK] Seq=1 Ack=1 Win=17520 Len=0	
127 13.594677		129.67.102.78	TCP	1043 > 1025 [ACK] Seq=3481 Ack=1106 Win=16415 Len=0	
128 13.601528		129.67.102.78	LDAP	searchRequest(1) "" baseObject	
129 13.602486 130 13.602528		129.67.102.73 129.67.102.73	TCP LDAP	[TCP segment of a reassembled PDU] searchResEntry(1) ""	
131 13.604748		129.67.102.78	TCP	1047 > 1dap [ACK] Seq=351 Ack=2185 Win=17520 Len=0	
132 13.614846		129.67.102.78	LSA	LsarLookupNames4 request	
133 13.615484		129.67.102.73	LSA	LsarLookupNames4 response	
	129.67.102.73	129.67.102.78	KRB5	TGS-REQ	=
135 13.618313		129.67.102.73	KRB5	TGS-REP	
136 13.619778		129.67.102.78	LDAP	bindRequest(3) sasl	
137 13.621265		129.67.102.73	LDAP	bindResponse(3)	
138 13.659691	129.67.102.73	129.67.102.78	LDAP	<pre>searchRequest(4) "DC=oucs-test,DC=ox,DC=ac,DC=uk" wholeSubtree</pre>	
139 13.660364	129.67.102.78	129.67.102.73	LDAP	<pre>searchResEntry(4) "DC=oucs-test,DC=ox,DC=ac,DC=uk"</pre>	
140 13.668179		129.67.102.78	тср	1049 > ldap [SYN] Seq=0 Len=0 MSS=1460	
141 13.668503		129.67.102.73	TCP	ldap > 1049 [SYN, ACK] Seq=0 Ack=1 Win=16384 Len=0 MSS=1460	
142 13.668835		129.67.102.78	TCP	1049 > ldap [ACK] Seq=1 Ack=1 Win=17520 Len=0	
143 13.672850		129.67.102.78	LDAP	bindRequest(7) sas1	
144 13.674239		129.67.102.73	LDAP	bindResponse(7)	
145 13.676791		129.67.102.78	LDAP	searchRequest(8) "" baseObject	
146 13.677117 147 13.677898		129.67.102.73	LDAP LDAP	searchResEntry(8) ""	
148 13.678386		129.67.102.78 129.67.102.73	LDAP	<pre>searchRequest(9) "CN=Default-First-Site-Name,CN=Sites,CN=Config searchResEntry(9) "CN=Default-First-Site-Name,CN=Sites,CN=Confic</pre>	
149 13.679293		129.67.102.78	LDAP	searchRequest(10) "cn=policies,cn=system,DC=oucs-test,DC=ox,DC=a	
150 13.680259		129.67.102.73	LDAP	searchResEntry(10) "CN={31B2F340-016D-11D2-945F-00C04FB984F9},CM	
151 13.739449		129.67.102.78	TCP	activesync > 1025 [ACK] Seq=1338 Ack=1057 Win=16464 Len=0	
152 13 745345		120 67 102 78	SMR	Trans? Demuest CET DES DECEDDAL Cile: \oursitest ov an uk	Ŧ
⊟ Kerberos TGS-R	EQ				
Pvno: 5					
MSG Type: TG	S-REO (12)				
⊕ padata: PA-T					
■ KDC_REQ_BODY Padding: 0					
-		rdable, Renewable)			
		i dabie, kenewabie)			=
	S-TEST.OX.AC.UK				
			2k1.oucs	-test.ox.ac.uk/oucs-test.ox.ac.uk	
till: 2037	-09-13 02:48:05 (Z)			

Nonce: 1918629348