



Active Directory and Oxford Single Sign-On

Bridget Lewis – ICTST
Adrian Parks – OUCS

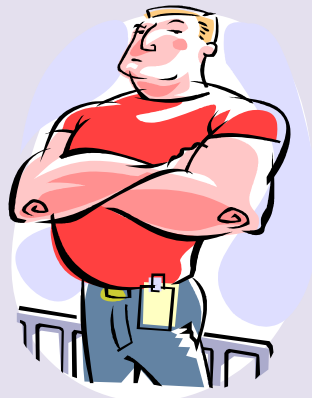
Aim

- 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



Fred A. Stair
Undergrad
Cornflake College



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

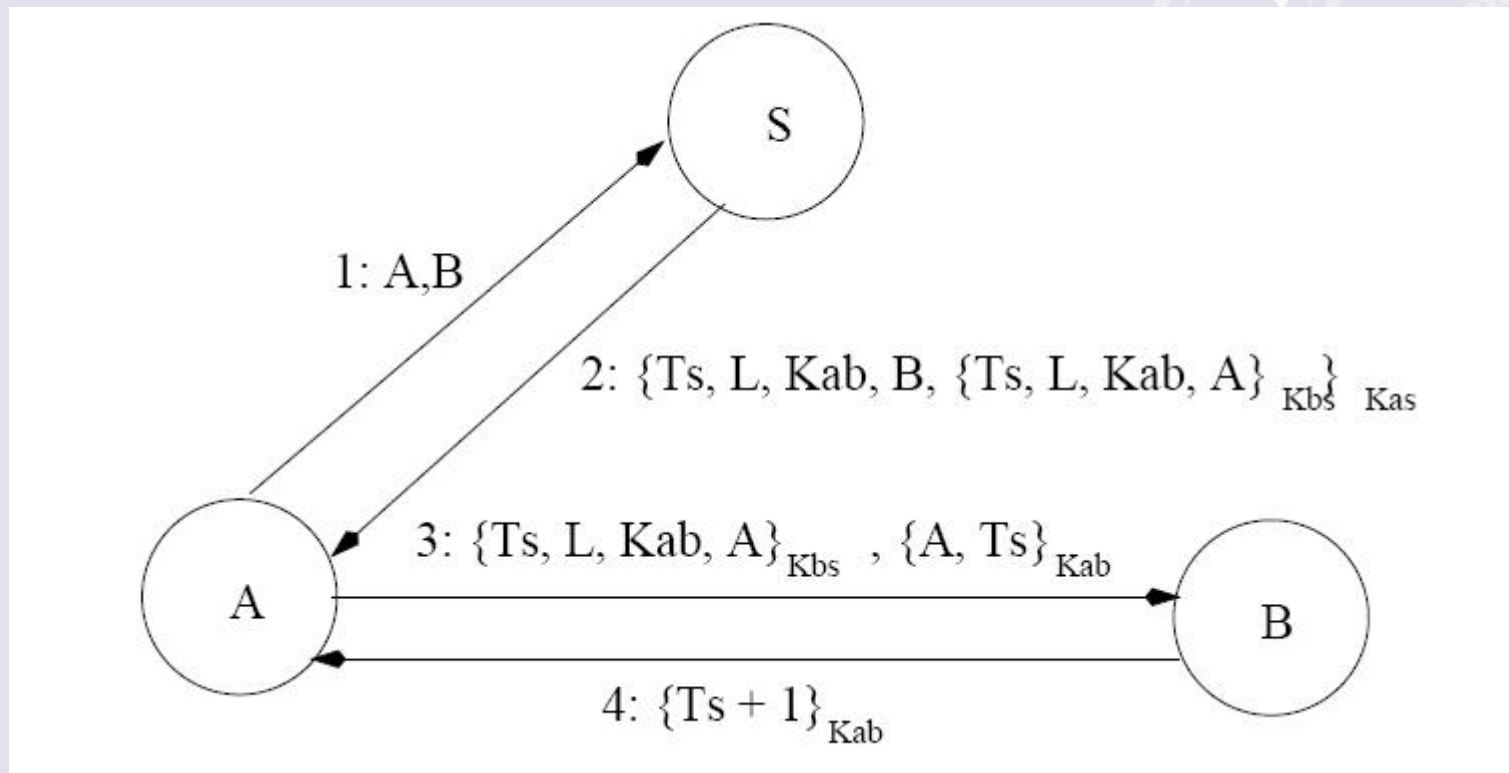
- Herald
- WebLearn
- Apache/IIS webservers (via Webauth)
- eDirectory
- Active Directory
- Open Directory

So how does it work...?

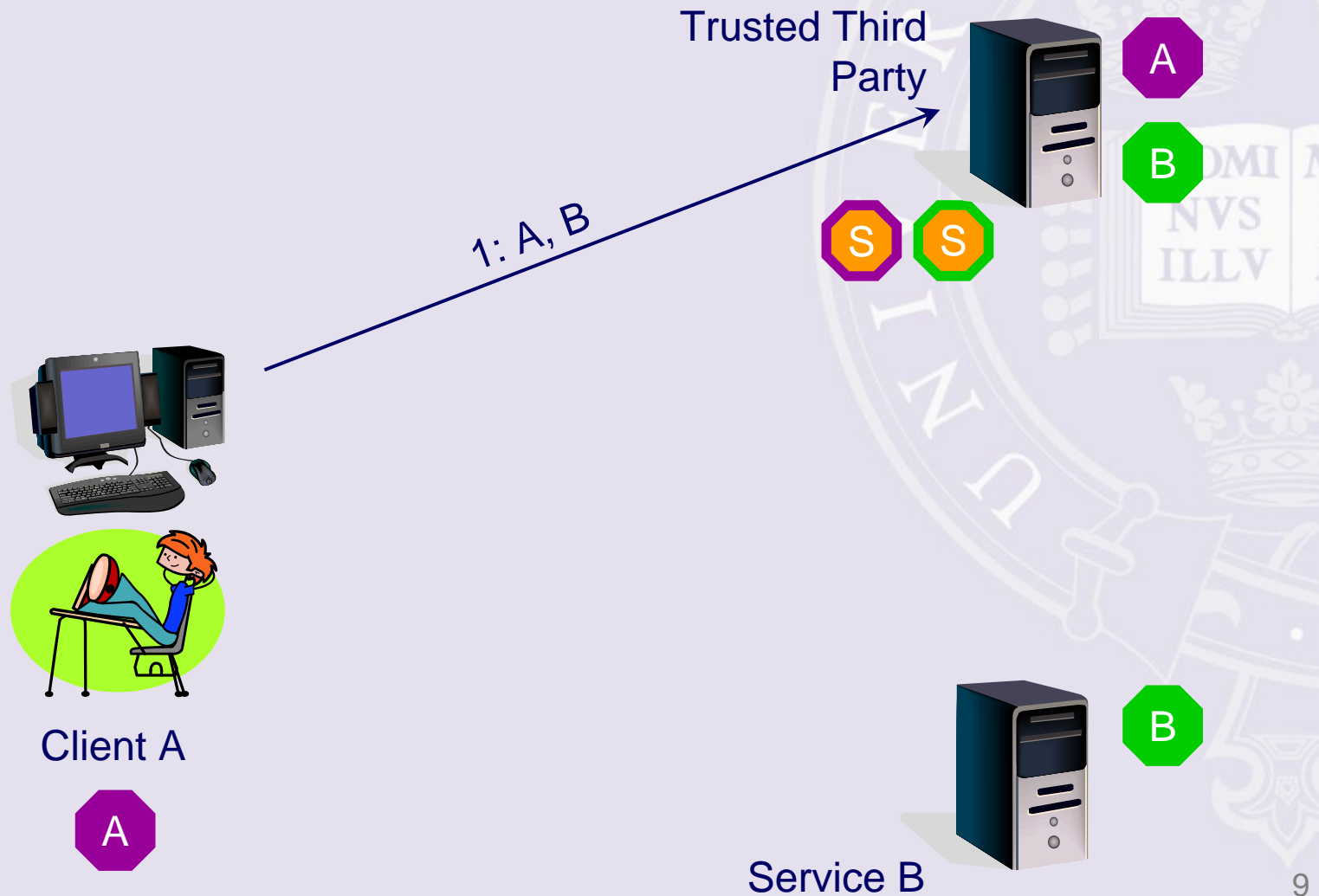
Simple, really...



Like this...



Basic Kerberos Functionality



Essential Terminology

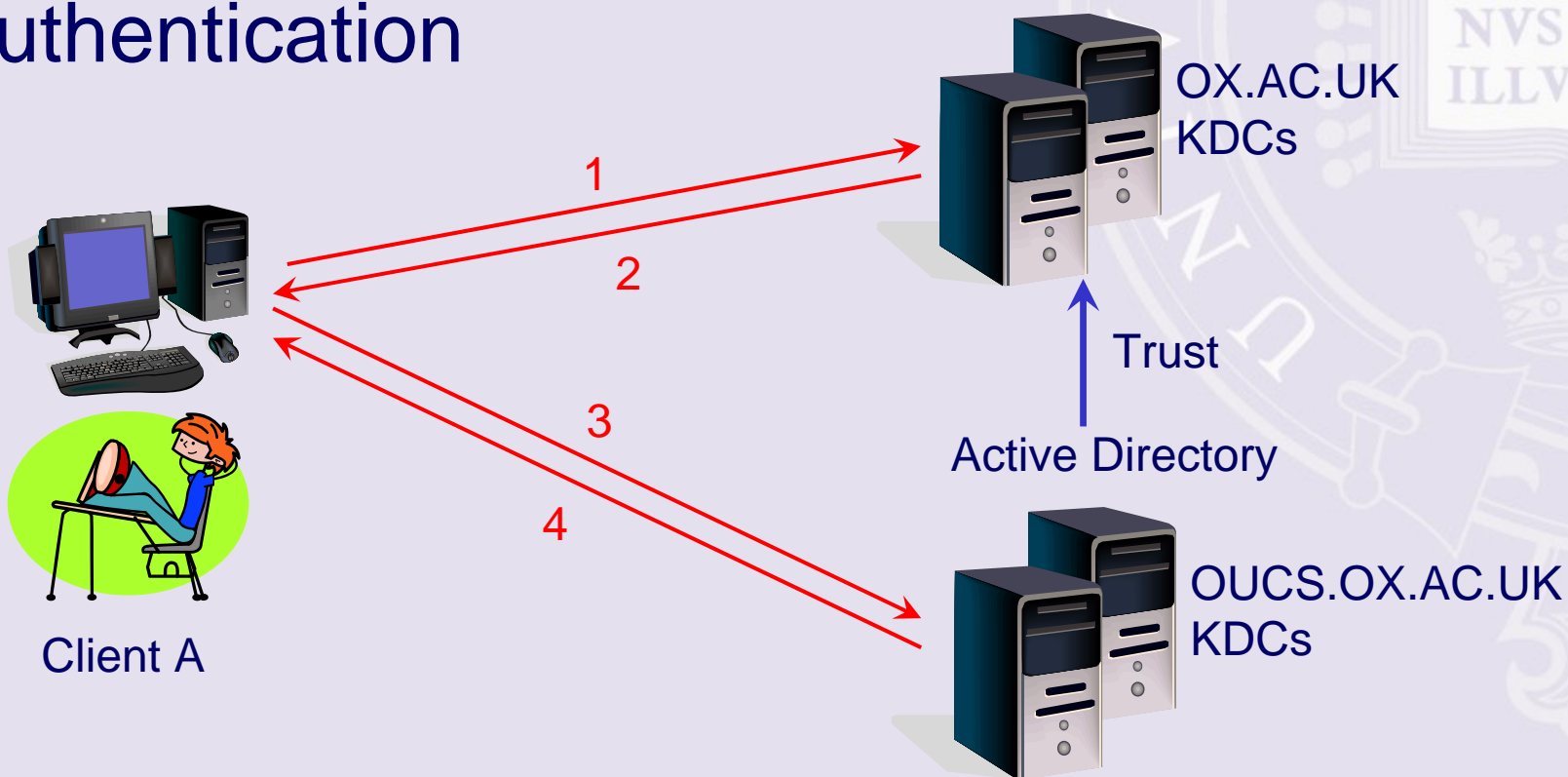
- Principal — user or service with credentials
- Ticket — issued for access to a service
- Key Distribution Centre (KDC) — issues tickets for principals in a realm
- Realm — set of principals in a Kerberos database, e.g. OX.AC.UK, OUCS.OX.AC.UK
- TGT (ticket-granting ticket) — confirms identity; used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



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.)

How do we set this up?

Full details are on the ITSS wiki:

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

How do we set this up?

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

See appendix for details!



How do we set this up?

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`

How do we set this up?

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:~$
```

How do we set this up?

4. Check time is in sync



How do we set this up?

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

```
ksetup /addkdc 0X.AC.UK kdc0.ox.ac.uk
```

```
ksetup /addkdc 0X.AC.UK kdc1.ox.ac.uk
```

```
ksetup /addkdc 0X.AC.UK kdc2.ox.ac.uk
```

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

How do we set this up?

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.

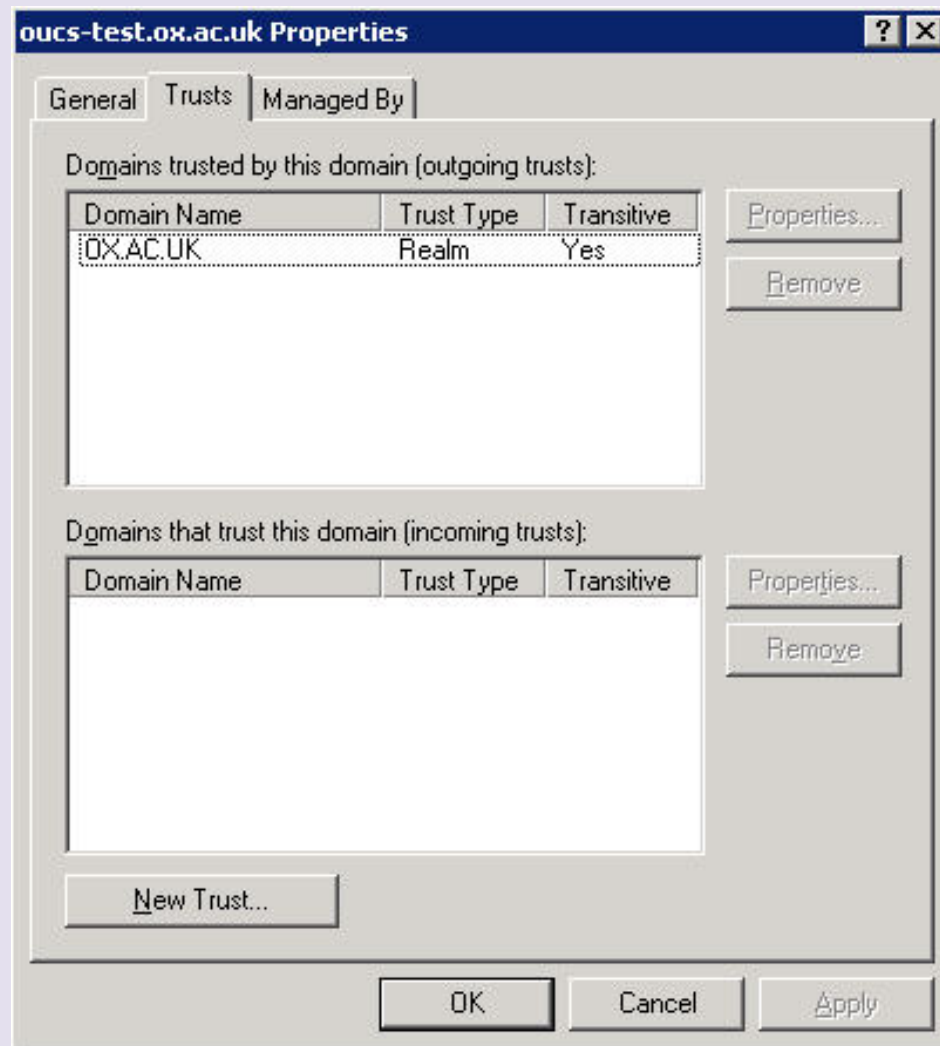
C:\Documents and Settings\administrator.STHUGHS>_

How do we set this up?

6. 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.

How do we set this up?



How do we set this up?

7. Check time is in sync



How do we set this up?

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

How do we set this up?



How do we set this up?

9. Reboot workstation and log in



Log On to Windows

Microsoft
Windows Server 2003 R2
Standard Edition

Copyright © 2005 Microsoft Corporation

User name:

Password:

Log on to:

OX.AC.UK (Kerberos Realm)
OX.AC.UK (Kerberos Realm)
STHUGHS

OK Cancel Shut Down 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

<http://web.mit.edu/kerberos/www/dialogue.html>

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

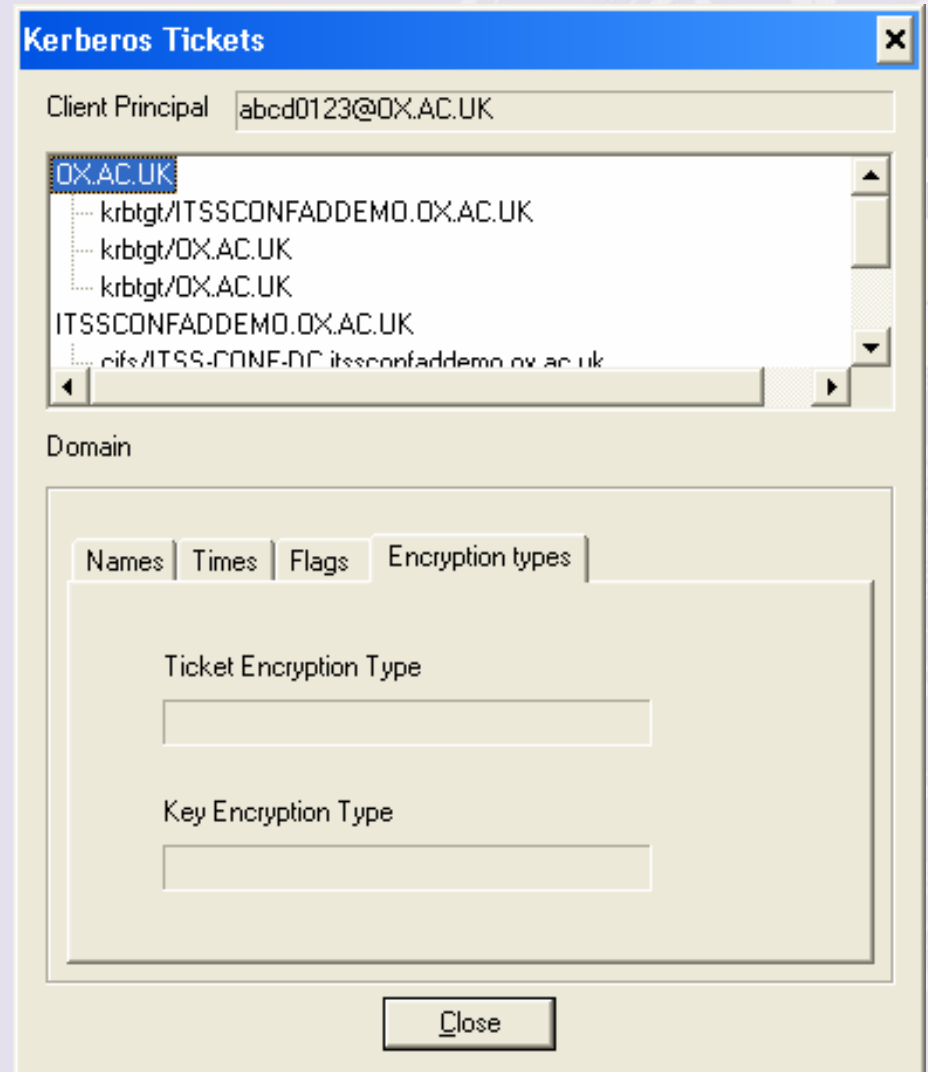
[1666237?ie=UTF8&s=books&qid=1182273864&sr=8-1](http://www.amazon.co.uk/Kerberos-Definitive-Guide-Jason-Garman/dp/0596004036/ref=sr_1_1/202-9173258-1666237?ie=UTF8&s=books&qid=1182273864&sr=8-1)

Appendix A — Utilities

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

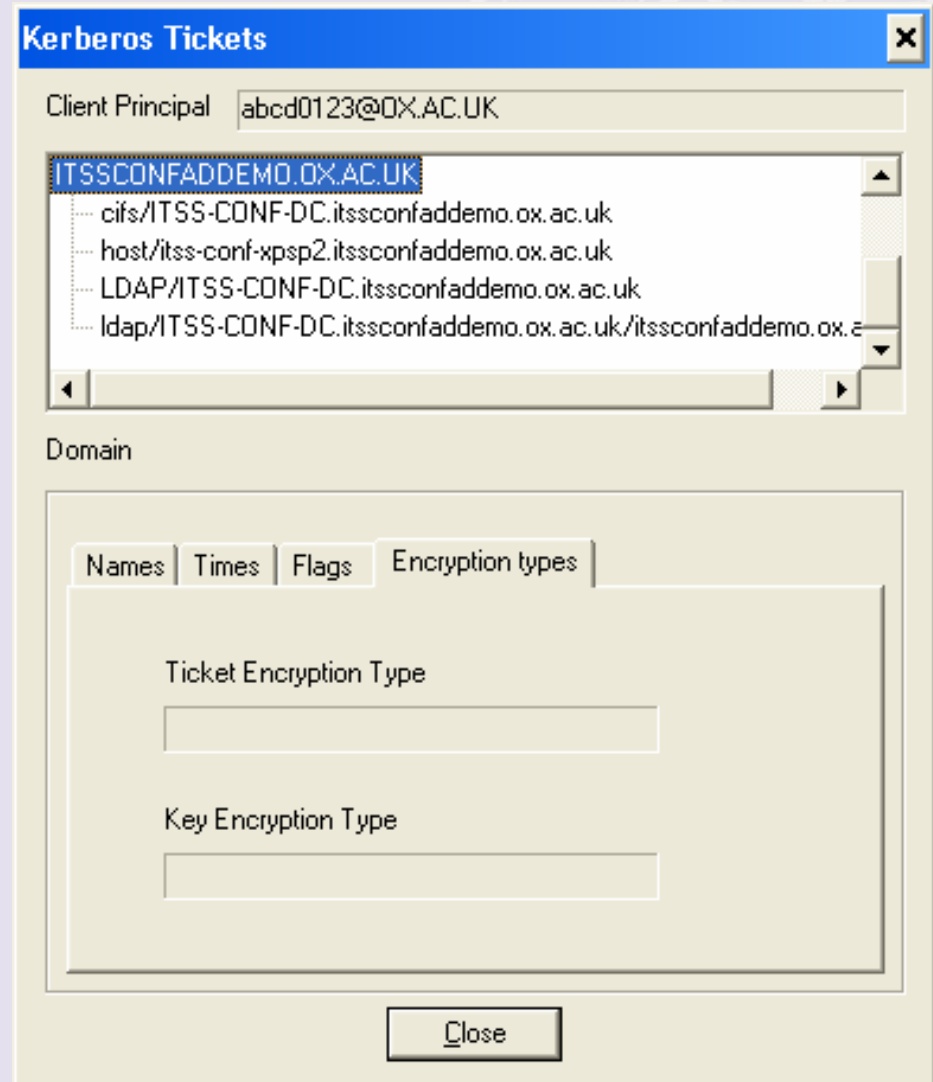
Kerbtray

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



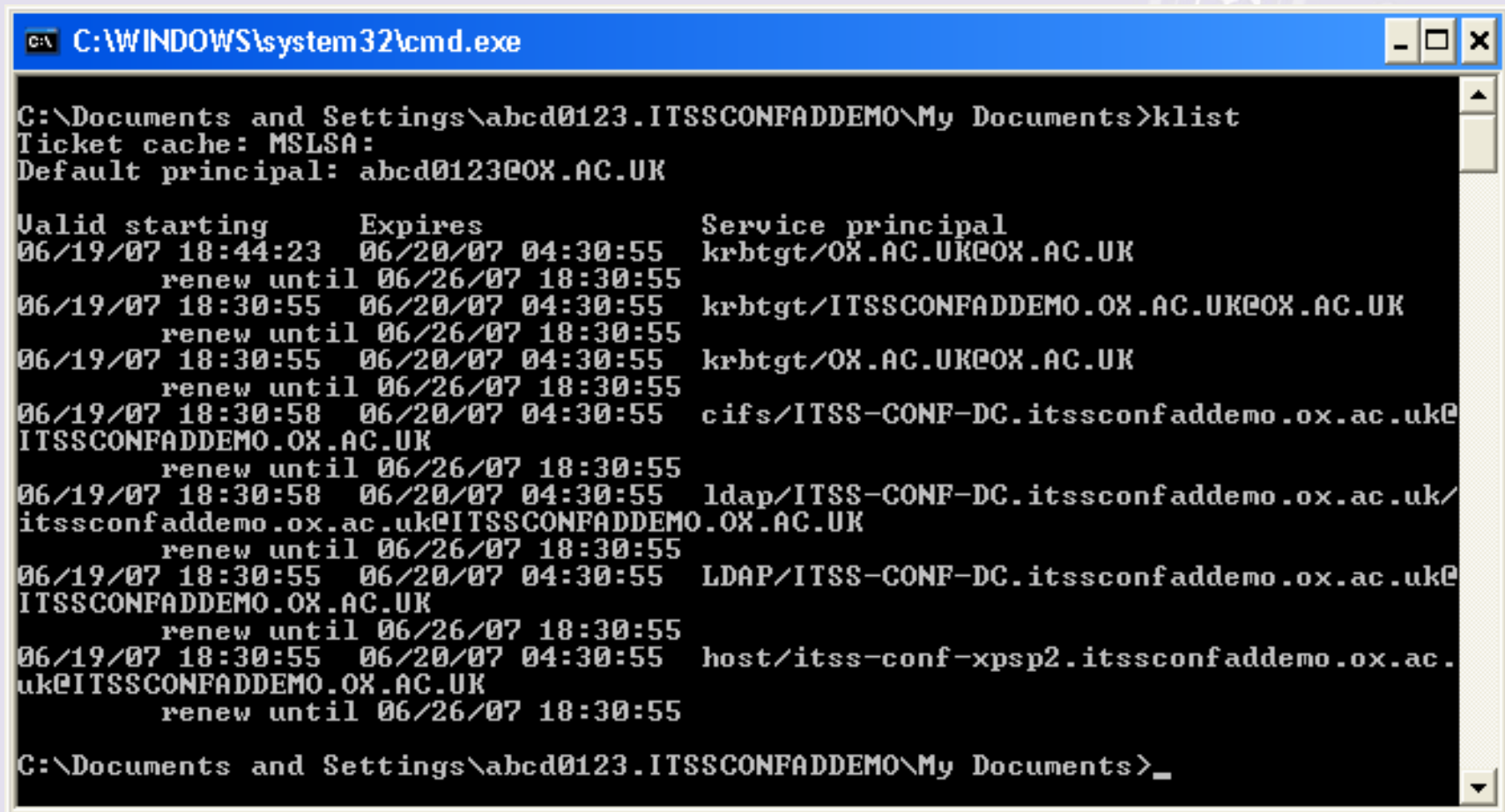
Kerbtray

- Picture shows tickets for services in Active Directory Realm



Klist

- Klist — as Kerbtray but command line



The screenshot shows a Windows command prompt window titled "C:\WINDOWS\system32\cmd.exe". The command prompt is running the 'klist' command, which displays the Kerberos ticket cache. The output shows the default principal and a list of tickets with their validity, expiration, and service principals.

```
C:\Documents and Settings\abcd0123.ITSSCONFADDEMO\My Documents>klist
Ticket cache: MSLSA:
Default principal: abcd0123@OX.AC.UK

Valid starting      Expires            Service principal
06/19/07 18:44:23   06/20/07 04:30:55  krbtgt/OX.AC.UK@OX.AC.UK
        renew until 06/26/07 18:30:55
06/19/07 18:30:55   06/20/07 04:30:55  krbtgt/ITSSCONFADDEMO.OX.AC.UK@OX.AC.UK
        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   06/20/07 04:30:55  ldap/ITSS-CONF-DC.itssconfaddemo.ox.ac.uk/
itssconfaddemo.ox.ac.uk@ITSSCONFADDEMO.OX.AC.UK
        renew until 06/26/07 18:30:55
06/19/07 18:30:55   06/20/07 04:30:55  LDAP/ITSS-CONF-DC.itssconfaddemo.ox.ac.uk@
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.ITSSCONFADDEMO\My Documents>_
```

Support Tools

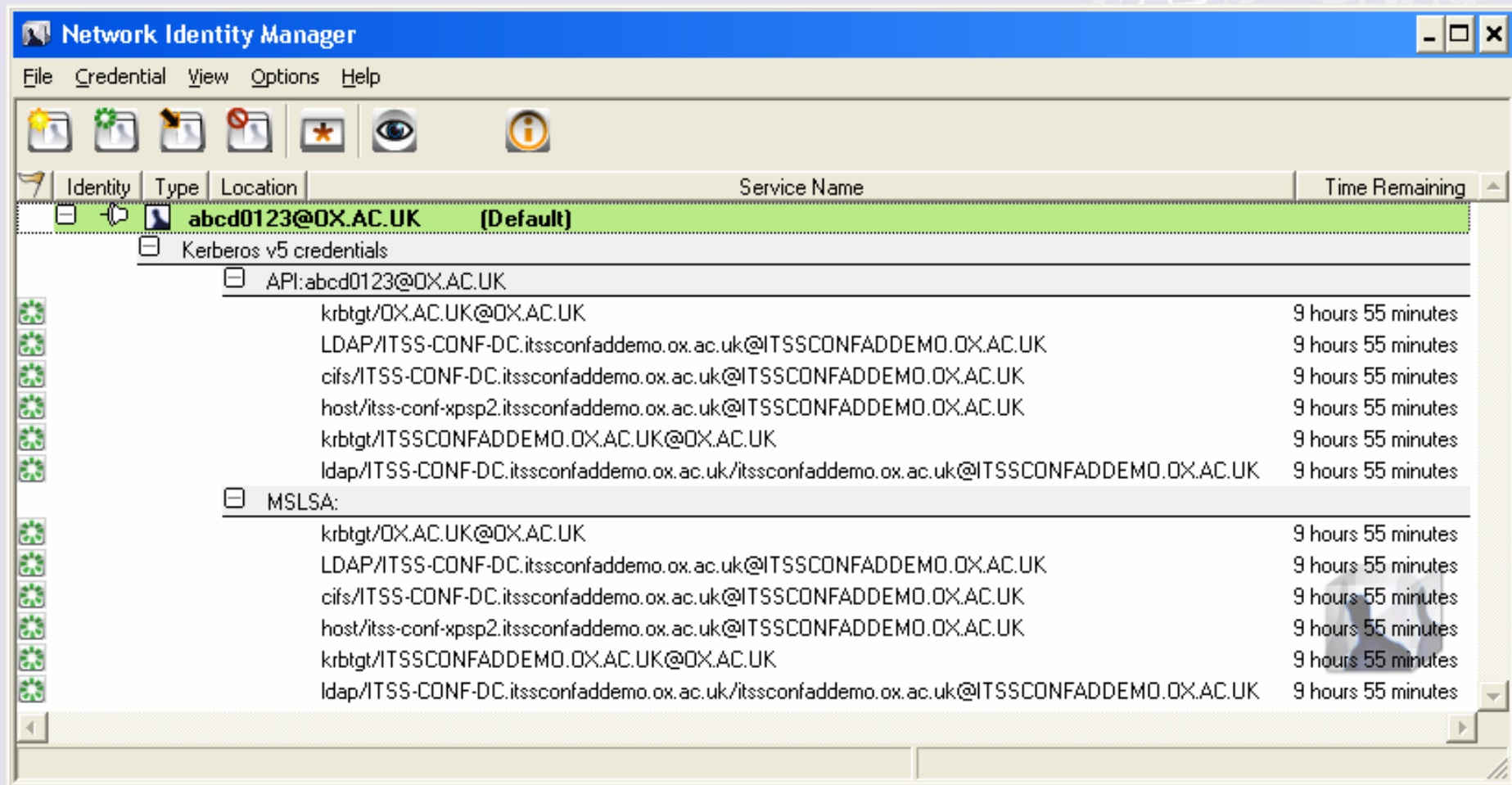
- Ksetup
 - Set up realm information
 - E.g. set KDCs for a given realm
- Ktpass
 - Manipulating principals



MIT Kerberos for Windows

- <http://web.mit.edu/kerberos/dist/>
- 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



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
 - <http://support.microsoft.com/default.aspx?scid=KB;EN-US;902336>

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`
 - <http://technet2.microsoft.com/windowsserver/en/library/ce8890cf-ef46-4931-8e4a-2fc5b4ddb0471033.mspx?mfr=true>

Automated Account Creation

- OUCS can provide nightly update of Oxford usernames and other information to each unit
 - http://www.oucs.ox.ac.uk/registration/card_data_2006.xml.ID=body.1_div.9
 - Use scripts to feed into Active Directory

Full Kerberos Functionality

KDC — 2 parts

AS: Authentication Server

TGS: Ticket Granting Server

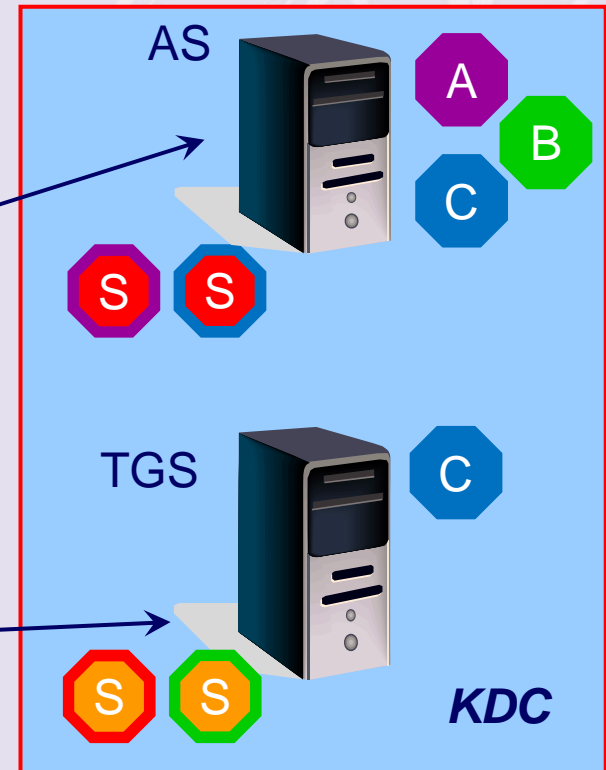


Client A



1: A, TGS

2: A, B



Service B

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



No.	Time	Source	Destination	Protocol	Info
48	2.740015	129.67.102.73	129.67.102.78	KRB5	AS-REQ
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	129.67.102.73	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\
59	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:
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
63	5.757103	129.67.102.73	129.67.102.78	DNS	Standard query A kdc0.ox.ac.uk
64	5.757588	129.67.102.78	129.67.102.73	DNS	Standard query response A 163.1.2.74
65	5.770367	129.67.102.73	163.1.2.74	KRB5	AS-REQ
66	5.774177	163.1.2.74	129.67.102.73	KRB5	KRB Error: KRB5KDC_ERR_PREAUTH_REQUIRED
67	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
69	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
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
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
75	7.554437	129.67.102.73	129.67.102.78	TCP	1042 > 1025 [ACK] Seq=1 Ack=1 win=17520 Len=0
76	7.556130	129.67.102.73	129.67.102.78	DCERPC	Bind: call_id: 1 LSA V0.0
77	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

☐ Type: PA-PAC-REQUEST (128)

☐ value: 3005A0030101FF

PAC Request: 1

☐ KDC_REQ_BODY

Padding: 0

☐ KDCOptions: 40810010 (Forwardable, Renewable, Canonicalize, Renewable OK)

☐ 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

No.	Time	Source	Destination	Protocol	Info
48	2.740015	129.67.102.73	129.67.102.78	KRB5	AS-REQ
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	129.67.102.73	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\j
59	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:
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
63	5.757103	129.67.102.73	129.67.102.78	DNS	Standard query A kdc0.ox.ac.uk
64	5.757588	129.67.102.78	129.67.102.73	DNS	Standard query response A 163.1.2.74
65	5.770367	129.67.102.73	163.1.2.74	KRB5	AS-REQ
66	5.774177	163.1.2.74	129.67.102.73	KRB5	KRB Error: KRB5KDC_ERR_PREAUTH_REQUIRED
67	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
69	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
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
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
75	7.554437	129.67.102.73	129.67.102.78	TCP	1042 > 1025 [ACK] Seq=1 Ack=1 win=17520 Len=0
76	7.556130	129.67.102.73	129.67.102.78	DCERPC	Bind: call_id: 1 LSA v0.0
77	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

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

Name: OX.AC.UK

No.	Time	Source	Destination	Protocol	Info
48	2.740015	129.67.102.73	129.67.102.78	KRB5	AS-REQ
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	129.67.102.73	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\j
59	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:
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
63	5.757103	129.67.102.73	129.67.102.78	DNS	Standard query A kdc0.ox.ac.uk
64	5.757588	129.67.102.78	129.67.102.73	DNS	Standard query response A 163.1.2.74
65	5.770367	129.67.102.73	163.1.2.74	KRB5	AS-REQ
66	5.774177	163.1.2.74	129.67.102.73	KRB5	KRB Error: KRB5KDC_ERR_PREAUTH_REQUIRED
67	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
69	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
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
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
75	7.554437	129.67.102.73	129.67.102.78	TCP	1042 > 1025 [ACK] Seq=1 Ack=1 win=17520 Len=0
76	7.556130	129.67.102.73	129.67.102.78	DCERPC	Bind: call_id: 1 LSA v0.0
77	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

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

No.	Time	Source	Destination	Protocol	Info
48	2.740015	129.67.102.73	129.67.102.78	KRB5	AS-REQ
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	129.67.102.73	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\j
59	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:
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
63	5.757103	129.67.102.73	129.67.102.78	DNS	Standard query A kdc0.ox.ac.uk
64	5.757588	129.67.102.78	129.67.102.73	DNS	Standard query response A 163.1.2.74
65	5.770367	129.67.102.73	163.1.2.74	KRB5	AS-REQ
66	5.774177	163.1.2.74	129.67.102.73	KRB5	KRB Error: KRB5KDC_ERR_PREAUTH_REQUIRED
67	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
69	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
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
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
75	7.554437	129.67.102.73	129.67.102.78	TCP	1042 > 1025 [ACK] Seq=1 Ack=1 win=17520 Len=0
76	7.556130	129.67.102.73	129.67.102.78	DCERPC	Bind: call_id: 1 LSA v0.0
77	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

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

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

till: 2037-09-13 02:48:05 (Z)

Nonce: 1865634814

```
Pvno: 5
MSG Type: TGS-REQ (12)
+ padata: PA-TGS-REQ
- KDC_REQ_BODY
  Padding: 0
  + KDCOptions: 40800000 (Forwardable, Renewable)
    Realm: OUCS-TEST.OX.AC.UK
  + Server Name (Service and Instance): ldap/nsmsw2k1.oucs-test.ox.ac.uk/oucs-test.ox.ac.uk
    till: 2037-09-13 02:48:05 (Z)
    Nonce: 1918629348
  - Encrypted Data: not here not here c1d not e1d des sha md5 des sha sha sha not here sha not here c1d sha
```