




Do Standards Help?

David Chadwick
d.w.chadwick@salford.ac.uk

24 October 2000 ©2000 JTM Consultancy 1

In the beginning...

- ☞ There was chaos
 - Many proprietary directories e.g. Banyan Vines, Netware Bindery and Email based address books e.g. Notes Name&Address Book
- ☞ Then along came an International Standard
 - ☞ X.500
- ☞ Which promised to unify them all



24 October 2000 ©2000 JTM Consultancy 2

And it sort of worked

- ☞ Paradise system (1991-94)
 - ~600 DSAs, 4,000 organisations, 1.25M entries
- ☞ NameFLOW-Paradise (94-99)
 - number of organisations kept rising
- ☞ EEMA directory challenge (1997)
 - 9 countries, 31 organisations
- ☞ All global X.500 based systems
- ☞ DAP and DSP worked fine..... but



24 October 2000

©2000 JTM Consultancy

3

But not without problems

- ☞ Managing the Root Context is very time consuming and no standard protocol for it
- ☞ Standard Access Control Scheme is too complex for many administrators to understand
- ☞ One level searches across system boundaries are slow
- ☞ Replication (DISP) is problematical
 - Standard has far too many options
 - EWOS profile has defined 6 different subsets
 - But only the simplest replication (copy everything!!) can be got to work between different suppliers



24 October 2000

©2000 JTM Consultancy

4

Why??

- ☞ Vendors usually sell into homogeneous environments i.e. one organisation
- ☞ Vendors want lock in i.e. the customer to buy all future directory systems from them
- ☞ The large scale heterogeneous distributed environment is only a small business segment
- ☞ So little incentive for vendors to spend resources on standard features to enable interworking in large scale distributed heterogeneous directory systems



24 October 2000

©2000 JTM Consultancy

5

Enter LDAP - a great leap forwards

- ☞ Much wider vendor support than X.500 protocols (all the big names claim support)
- ☞ Simple APIs and toolkits, often free, encourage lots of development work
 - e.g. free Java API from the Internet
- ☞ For simple directory access it is the answer



24 October 2000

©2000 JTM Consultancy

6

Or is it a giant leap backwards?

- ☞ Can't replicate between vendors - no standard access controls, no replication protocol
- ☞ Can't easily build distributed systems
 - no chaining, no standard knowledge references
 - X.500 Paradise was doing this 10 years ago
- ☞ EEMA challenge did these in 1997 with X.500



LDAP Administrator



24 October 2000

©2000 JTM Consultancy

7

Conclusion?

- ☞ LDAP is fine as an access protocol to individual directory servers
- ☞ But it cannot currently handle the tough jobs of distribution and replication
- ☞ But is the former even true?



24 October 2000

©2000 JTM Consultancy

8

LDAP is not without its major problems either

- ☞ LDAPv2 is dead - IETF has stopped its standardisation
 - Cannot update it (not extensible)
 - Cannot interwork with future versions e.g. LDAPv3
 - No support for distributed directories
- ☞ LDAPv3 has cancer
 - Infinitely extensible



24 October 2000

©2000 JTM Consultancy

9

Need an extension to LDAPv3? Then invent a draft standard yourself

- ☞ Example of directory synchronisation
 - Innosoft's Triggered Search Control
 - ◆ Connection stays open after Search Results returned and updates continue to flow
 - Microsoft's Active Directory Synchronisation
 - ◆ Passes a cookie between server and client
 - Netscape's Persistent Search Control
 - ◆ More sophisticated version of Triggered Search
- ☞ Now IETF is standardising LDAP Client Update Protocol (LCUP) to replace all 3. OR WILL IT?



24 October 2000

©2000 JTM Consultancy

10

Some statistics (courtesy of Colin Robbins)

- ☞ By Oct 99 we had approx 15 RFCs related to LDAP
- ☞ We also had at least 25 IDs relating to proposed extensions
- ☞ There are also 10 or so other related IDs
- ☞ A quick survey suggests an average size of 10 pages
- ☞ So in total, we have approx 500 pages of standard and proposed standards related to LDAP. This is being added to all the time
- ☞ For comparison purposes X.500(93) has 9 documents comprising just over 400 pages
- ☞ **Is X.500 (93) a lightweight variation of LDAP?**



24 October 2000

©2000 JTM Consultancy

11

Even worse, do your extension in a non-standard way

- ☞ For example, when doing a one level Search beneath a country entry, do not return referrals to the servers holding the organisation entries, but return copied details from those entries. When doing a full subtree Search, do return the referrals rather than the copied information. This has been implemented by one supplier as a configuration parameter in the LDAP server



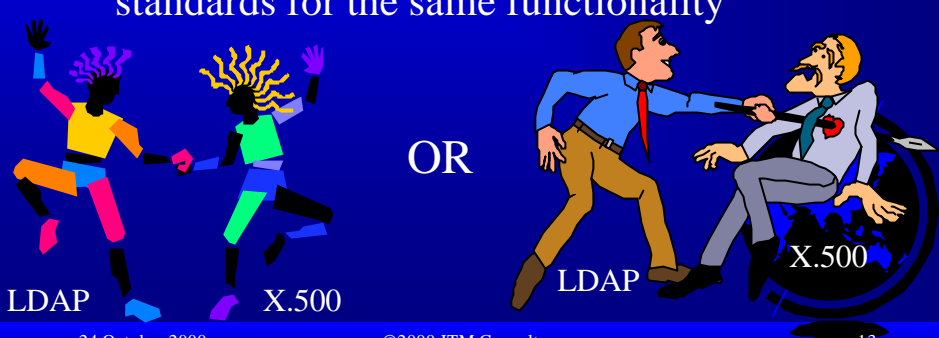
24 October 2000

©2000 JTM Consultancy

12

Religious Wars? IETF vs. ISO

- ☞ Not invented here syndrome
- ☞ Culture of doing things differently
- ☞ Leads to re-inventing the wheel and multiple standards for the same functionality




OR

24 October 2000 ©2000 JTM Consultancy 13



IETF Standardisation Process

- ☞ Must reach rough consensus
- ☞ Anyone can participate, but its **very time consuming**
- ☞ Some vendors have been known to purposefully slow down the process by raising technical objections
- ☞ Requires at least two independent interoperable implementations and some operational experience before an RFC can reach Draft Standard status
 - LDAPv2 took 7 years to reach Draft,
 - LDAPv3 took 4 years to Proposed Standard, still not Draft
 - Authentication Methods took 2 more years (May 2000)
 - Access controls - we are still waiting



24 October 2000 ©2000 JTM Consultancy 14

Software lifecycle

- ☞ Invent, improve, maintain, fade out
- ☞ Eventually you get spaghetti, that is too costly and difficult to maintain 
- ☞ Applies to standards as well
- ☞ E.g. X.509 - similar but different extensions that do similar but variations of the same thing
 - CRL scope vs. Issuing distribution points, Delta CRL and Base Update time extensions
- ☞ Number of defects in standards and complexity rises to unmanageable levels 

24 October 2000 ©2000 JTM Consultancy 15

X.500 (2001) - a bridge too far?

- ☞ X.500 (2001) is horribly complex. Added
 - compound entries, families of entries, hierarchical groups, matching relaxation and tightening, search rules
- ☞ Not even all of 1993 standard has been implemented yet by vendors
- ☞ And most of 1997 standard never will be
- ☞ Could 2001 be the lead weight that breaks the camel's back 

24 October 2000 ©2000 JTM Consultancy 16

Dominant Suppliers

- ☞ Like to set their own standards
 - Classic example - Microsoft's ADSI when we already have a standard LDAP API from the IETF
- ☞ Like to modify de-jure standards to fit their own purposes
 - Classic example - both Microsoft and Netscape have modified the X.521 object class Top - DIFFERENTLY!!
 - Win2000 uses a modified Kerberos to prevent Win2000 clients using non MS servers whilst non MS clients can use MS servers



24 October 2000

©2000 JTM Consultancy

17

In conclusion

- ☞ Problems caused by the standards process
- ☞ Problems caused by too many standards
- ☞ Problems caused by vendors not implementing the standards
- ☞ Problems caused by dominant suppliers



24 October 2000

©2000 JTM Consultancy

18

A closing thought

- ☞ Maybe the best standard is when everyone uses the same product from the same supplier
 - e.g. Microsoft Office
- ☞ Remember the time when transferring documents between pan-European project teams was a nightmare



☞ SWEET DREAMS



24 October 2000

©2000 JTM Consultancy

19