

UNIX and Open Systems Users Group (AUUG) on the one hand, and Microsoft on the other.

AUUG emphasised that the use of standard, open protocols across a network allowed a wide range of software, hardware and communications products to interact successfully. If reliance were placed on one proprietary, closed source application, such as Microsoft Word, then all other users were committed to using that same product if they wished to have access to the data.

AUUG argued that independence from a particular vendor was an advantage. As cited the report, AUUG urged that: "Software vendors may go out of business, may increase prices to an unacceptable level, or may decide that it is no longer in their business plan to support the software". In the long term, this could lead to data becoming inaccessible.

Microsoft countered by asserting that data stored in its closed format would still be accessible in 100 years time and that it was in the company's best interest that compatibility was maintained so that customers could see value in upgrading to a new version and could be confident that they would have the ability to bring forward their documentation.

On the specific question of the security merits of open source software compared with closed source software, AUUG stated that "... access to source means that an enormous amount of peer review goes on" and that "... the fact that it is available means that it is looked at by a very broad number of people from different educational and cultural backgrounds, and that diversity leads to a lot of, out-of-the-box thinking; therefore a lot of problems are found proactively and are fixed".

Microsoft countered this argument by saying that security requires highly qualified experts to actually examine, fix and test code. It claimed that simply making source code available to volunteer programmers was not enough, and widespread source code availability itself could introduce security risks.

The committee concluded that "the debate between the proponents of closed and open source software seems likely to continue with no decisive advantage to either side" and that there were strong arguments for both sides of the debate. Nevertheless the Committee considered it appropriate to acknowledge and highlight a specific summary comment by AUUG:

"[AUUG] ... would hope that the

government would make the best technology choice at every juncture. Sometimes the best technology choice may indeed be a proprietary system. It may provide features, capabilities or some functionality that is only available with that system. However, AUUG feels that the government should seriously consider using open systems, particularly where equivalent functionality is available at a much lower cost and with all the benefits of open source software."

Regulation of .eu domain names

The registration process for the .eu domain names is due to commence later this year. Any individual who is resident within the EU, any undertaking having its registered office, central administration or principal place of business within the EU and any organisation established within the EU will be able to register .eu domain names.

The .eu domain names are not intended to replace the current national ccTLDs of EU Member States. However, they will provide users with the opportunity

of having a pan-European identity for their websites and e-mail addresses. The European Commission is responsible for putting in place the necessary steps for the implementation of the .eu TLD. The European Registry for Internet Domains ("EURID"), a private sector, non-profit organisation, will be responsible for the day-to-day management and operation of the .eu domain. It is hoped that EURID will be ready to commence with the registration process in the second half of 2004. Certain restrictions will be

enforced to avoid abusive or speculative registrations such as a sunrise period allowing those holding prior rights to a name to register it prior to the general registration process commencing. Furthermore, public bodies will also have the opportunity to register their names in advance of the general public.

(This article was supplied courtesy of Vanessa Shield, Linklaters IT & Communications, Intellectual Property News, Issue 27, March 2004.)