LEVEL 5: WHAT SHOULD IT DO?

George D.M. Ross 10/12/85

In the "File Access Protocol" document of 03/12/85 it was suggested that there should be a protocol layer sitting between those layers responsible for providing a reliable transport service and the layer responsible for interpreting and acting on users' requests, whose job would be to establish the identity of the user at the other end of the connection making the requests. By making himself known, once, to the environment which the entities of this protocol layer constitute, the user's identity would thereafter automatically become known to any facility which he attempted to access, without there being any further requirement for him to log on separately to each such facility. As well as file servers, we might envisage interactive access to multi-access systems and mail servers being among the facilities which might be accessible in this way. In this document we consider how such an environment could be implemented. See also the document "Network Access Protocol" of 21/11/85, which discusses this protocol but without the added refinement of the domains of accreditation necessary for working in a wider environment.

Note that we are concerned here solely with the activities of the level 5 entities. Level 4 downwards does not concern us, neither does level 6 upwards.

In order to establish his identity, the user must quote a username and password to some authorising agent in the environment, in exchange for which he will be issued with a unique identifier. This identifier may be valid globally, or it may be valid only locally in which case the user must subsequently use it to obtain a globally valid token. In either case, when the user wishes to access some facility he quotes the globally valid identifier (the authorisation token) to that facility, together with the identity of the authorising agent which issued it.

When the target facility receives one of these authorisation tokens it must first of all decide whether the authorising agent which the user claims issued the token is one of those which it is prepared to believe in. If the issuing authorising agent's identity is acceptable, the target facility then presents the authorisation token to that authorising agent for validation, receiving in return the name by which the user identified himself to the issuing authorising agent.

The target facility can now consider the user's identity together with the identity of his authorising agent in order to translate the username from the authorising agent's domain of accreditation into the user's true identity in the facility's own domain of accredication. It can do this locally, either by table lookup or algorithmically, or by consulting a a server on the network whose job it is to perform such translation, or by some other means. Such a translation is necessary because there may be several servers accessible to the user, all of which are under the control of different management; in order that conflicts of identity should be avoided, each username must be qualified by the identity of the domain of accreditation in which it is valid, and then converted to the local domain of

accreditation for the convenience of the target facility.

Finally, the facility can now permit or deny access, based on the user's true identity and, perhaps, the identity of the client which is acting as the user's intermediary. Thereafter the higher protocol layers can conduct their dialogue, with the identity of the user being implied by the connection just established.

The format of the authorisation tokens is for each authorising agent to decide. However, they should be chosen from a large enough name space that they are hard to guess or forge, and they should have a limited lifetime in order further to enhance security.