nition convention. *See* OPEN SYSTEMS INTERCONNECTION.

X.400. In data communications, a standard for electronic mail interchange. *See* ELECTRONIC DATA INTERCHANGE, ELECTRONIC MAIL.

Y,Z

Younger Committee. A UK committee that considered the problems of data protection and privacy and reported in 1972. *See* DATA PROTECTION, PRIVACY.

Z. In electronics, the symbol for impedance. *See* IMPEDANCE.

zeroization. In computer security, a method of degaussing, erasing or overwriting electronically stored data. *See* DEGAUSS, ERASURE, OVERWRITING.

zero knowledge proof. In authentication, a technique by which two parties can authenticate each other, but an eavesdropper would be unable to impersonate as one of the parties, irrespective of the number of authentication dialogues known to the eavesdropper. The two parties must share some secret information.

A simple example would be two people who wish to hold a public conversation and one of them has taken a certain action (e.g. paid a bill at a restaurant). However, they do not wish to reveal to any third party which one had taken the action. The two parties toss a coin, and observe the result, while hiding the coin from others. They then call heads or tails. The person who paid the bill will call the true result of the coin toss, while the other who did not pay the bill will call the opposite result. If the two calls are different then each will know that the bill has been paid, exactly once, but an onlooker would be unable to detect the payee. *See* FIAT SHAMIR ALGORITHM.

zone encryption. *Synonymous with* NODE ENCRYPTION.