Distributed Systems SOLN. NOTES · Paper 9 2013

2004 P9 Q4 JMB

a) University Dept file service behind firewall
All principals are locally named and registered, as are groups and group membership.
4 Authentication is of principals.
An access control list can be held for each file ... (usual).

b) Commercial Internet-based file service
No global registration of principals is available.
On uploading the file the owner could be returned an encryption-protected (and paying) capability and must present this in order to access the file. This should be principal-specific to guard against theft. Authentication of principal
8 can be via a PKI. A principal-specific capability authorising read should be given to other principals.

c) Sales data in worldwide company
Here, employees come and go and roles are easier to manage, in this case, SalesDepartment member. A principal needs to prove its right to use the role. A role certificate might be used but revocation is important (when someone leaves or is delegated).
8 X.509 attribute certificate might be allocated annually and a revocation list held.

d) EHRs in a nationwide service
Here we need to represent principals, relationships and roles. Parametrised roles meet the need, for example qualified-doctor(BMA-ID), employed-doctor(hospital-ID, doctor-ID) treating-doctor(doctor-ID, patient-ID). As above we need some
8 form of PKI-based authentication and proof of role membership. System may distinguish persistent credentials and session-activated (transient) roles.

e) Solution to online coursework
Here, roles are setter(course-ID), candidate(course-ID).
Authentication - as for above. RBAC must justifiable for courseware re-usable by different distributed universities.
8 New aspect is the time constraint - access depends on where we are in the workflow.

a and 2 other parts:
They will give more details for the 2 selected parts.
Alternative solutions are possible - must be justified.