Ticket-based access control for VOStore?

Guy Rixon

March 2005

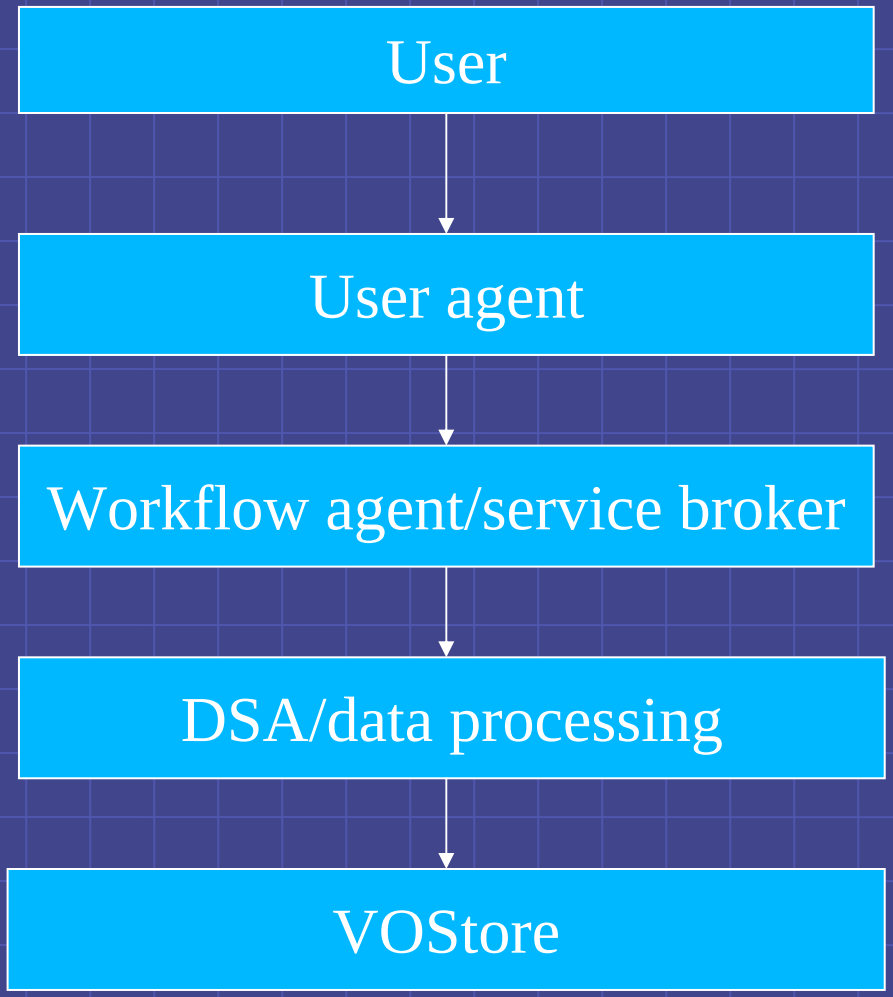
We hold the following to be self-evident…

- VOStores need to be secure against misuse
- We want a single-sign-on system
- We have astro communities as sign-on points
- We want global interoperablity of VO stuff
- We want to interoperate with other systems (grid, D-Space, SRB, etc.)
- We (sometimes) want to do automated stuff
- We want detailed control of user privs
- Security is not simple!

Basic requirements

- Data are owned
  - Do only operations authorized by data owner(s)
  - E.g. check CRUD permissions
  - E.g. check user's share of group quota
- Storage is owned
  - Do only operations authorized by storage owner(s)
  - E.g. check user membership of authorized group
  - E.g. check group quota

Delegation chain



User never talks to VOStore directly.

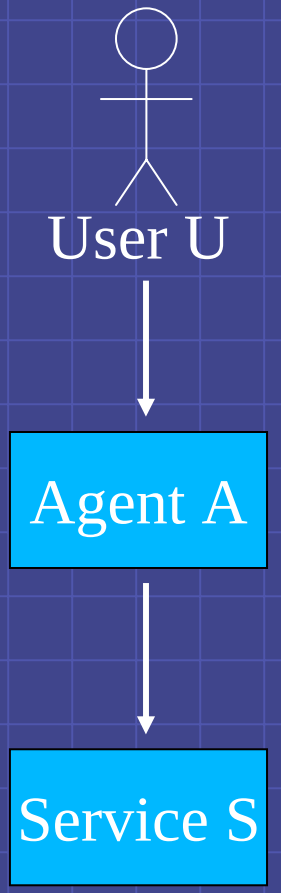
Hence, need to associate chain of agents with user's will to use VOStore

Identity delegation

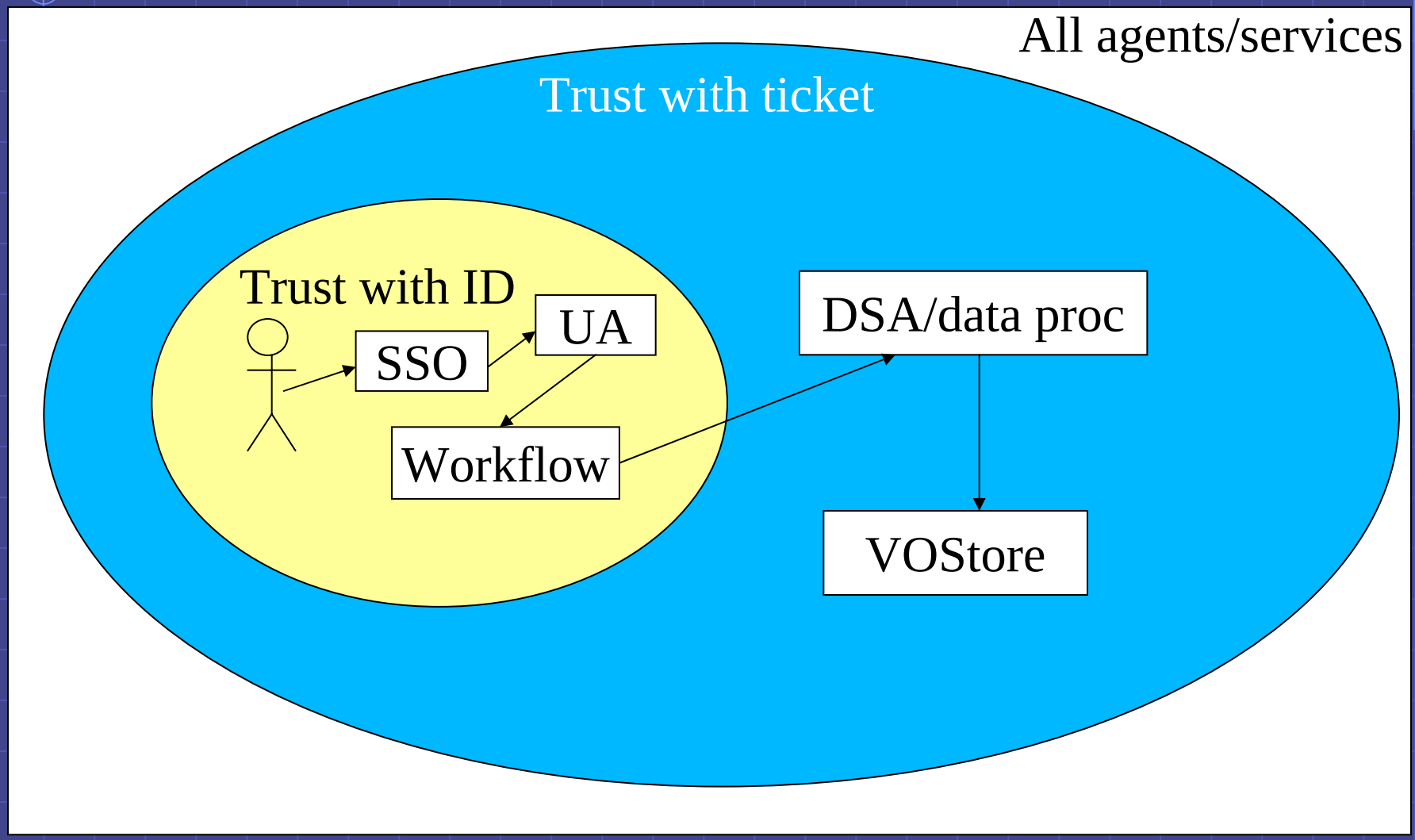
- Service S trusts user U.
- U trusts agent A.
- **U lets A authenticate as U**.
- => S trusts U as much as A.
- => A can do anything U can to S.
- => A could misuse U's privileges.
- => U doesn't need to know which privileges are required.

Privilege delegation

- Service S trusts user U.
- U does not entirely trust agent A.
- **U gives A a ticket** authorizing a specific action.
  - Ticket is specific to A.
- A authenticates to S as itself.
- A gives S the ticket.
- => S allows A only the actions in the ticket.
- => A can't misuse U's privilege
- => U needs to know what tickets are required



Delegation: trust boundaries



Proposal

- Access to VOStores should be controlled by tickets.
  - Agents authenticate as agents, not as users.
  - Tickets link agent identity to user identity.
  - Tickets are warrants (digitally-signed statements).
  - Tickets have globally-unique-for-all-time names.
  - Tickets can express authorization constraints, e.g. quota usage managed by user group.
  - Special case: identity warrant delegates all privileges associated with user identity.

How to send a ticket to a service

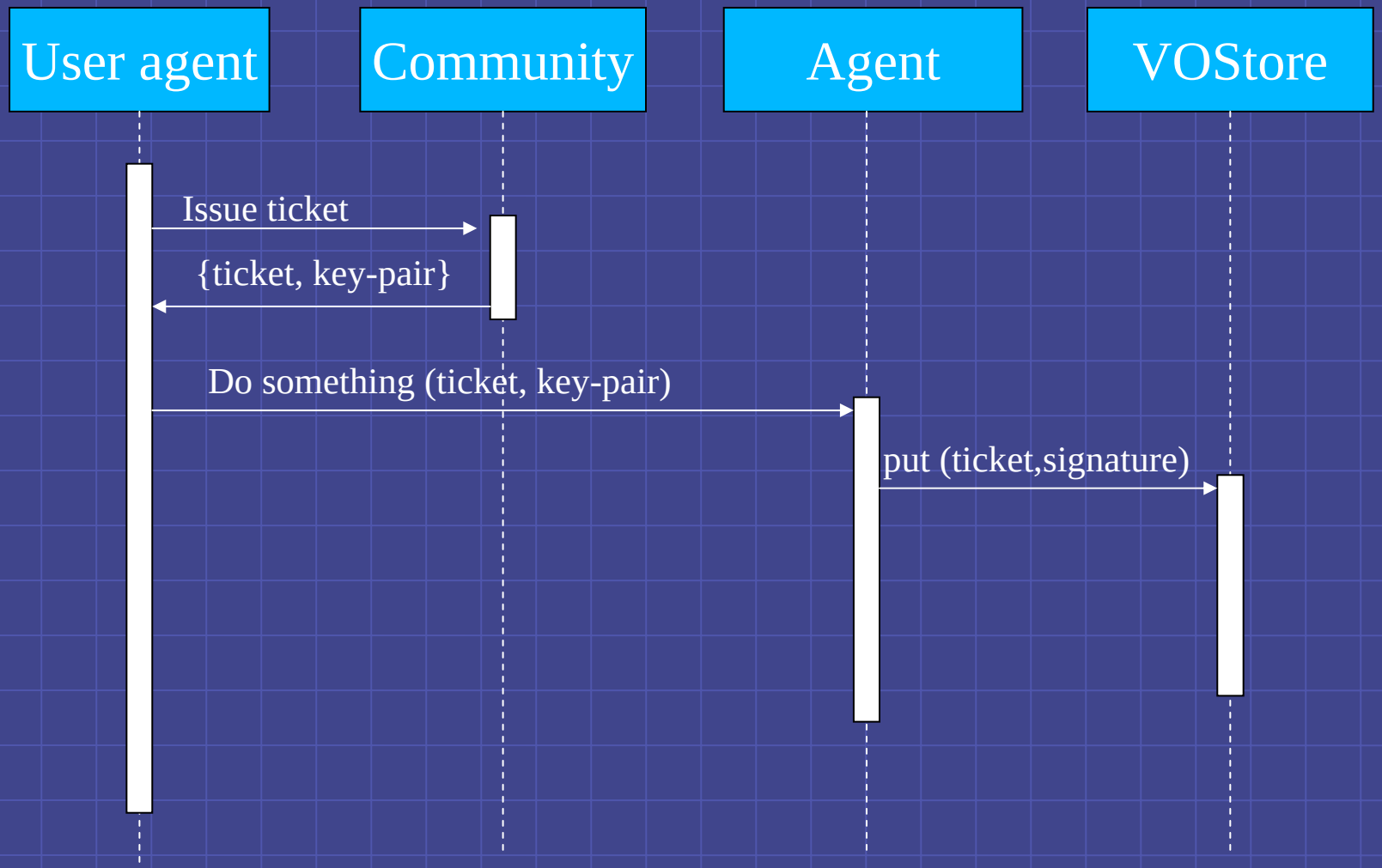
- Send the ticket with the request
  - Agent A puts text of ticket in request to service S.
  - E.g. WS-Security stuff in SOAP headers.
- Send the ticket in advance
  - Agent A1, trusted by service S, sends a ticket in respect of untrusted agent A2.
  - A2 gives name of ticket in request
  - Works for HTTP-get as well as SOAP.
- Use a referee
  - Agent A sends a ticket name and name of referee R, trusted by service S.
  - S gets the ticket from R.

Authentication redefined

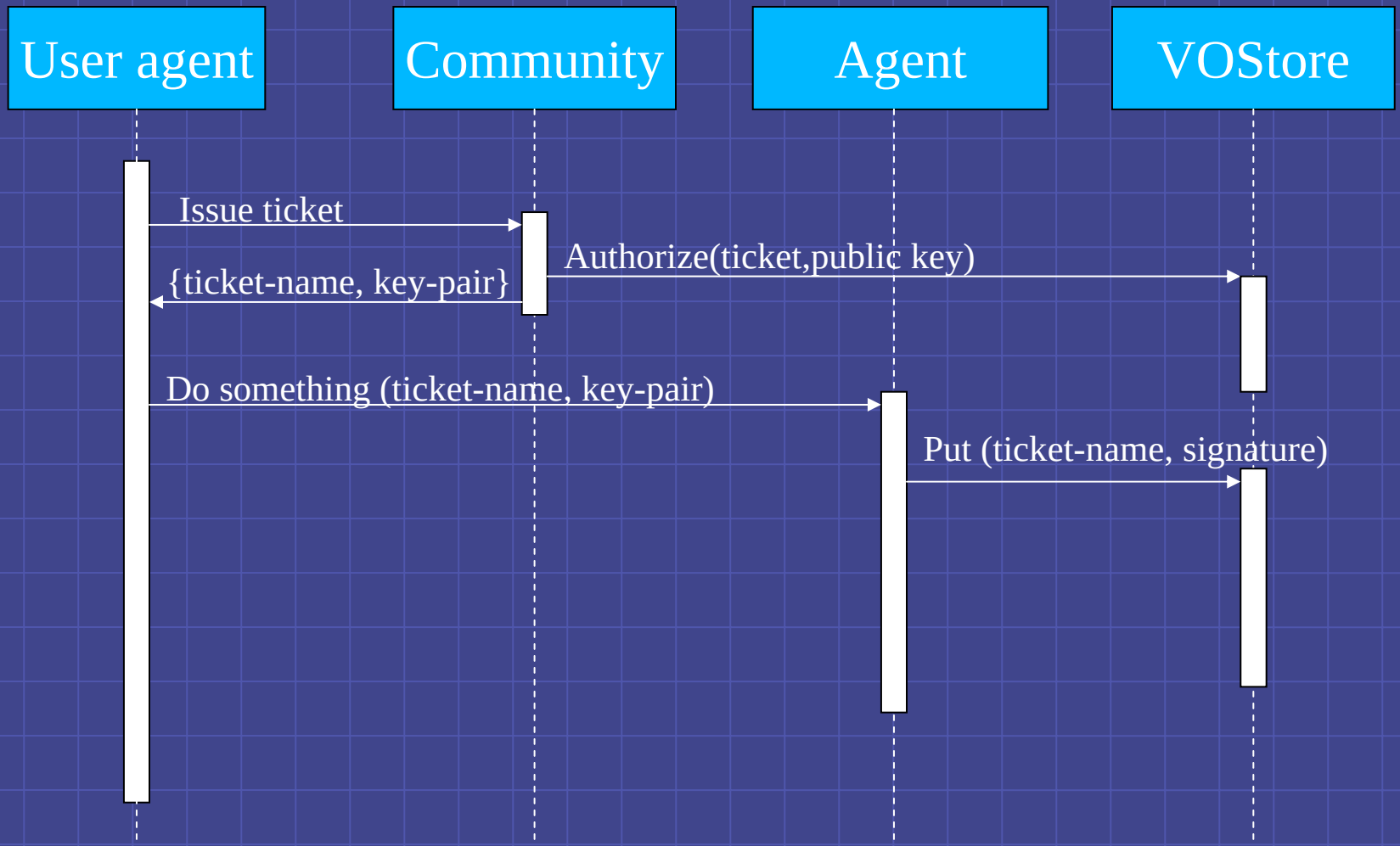
- Not:
  - Is this agent acting on behalf of the user?
- But:
  - Does this agent have a right to use the ticket?
- Two ways to check:

1. Ticket is associated with agent's crypto key-pair.
2. Name of ticket is a secret
   - Use the name as a temporary password.
   - Works best with single-use tickets.

Community as source of tickets (1)



Community as source of tickets (2)



Community as source of tickets (3)