Name and Identity

What is a name?
A designation. We used to assume name ←→ person/thing (1 to 1) – but not necessarily.

Lecture first (authentication, identity) – then look at flows – decision-making processes.

Are we going to focus on one user? Town Meeting? We'll decide within the next wk.
List of questions – today or tomorrow, by email.

Government sequence of adopting web technologies
(Increasing time and increasing complexity)
1. Publish – just give information
2. Interact – quick query – discussion board, etc.
3. Transact – business interaction – purchases. Link up to other organizations (credit cards). Identity becomes important.
4. Integrate – Put transactions together – diff organizations. Business hires someone – 7 different agencies in MA. Fill out one form on front end – redistributes. Faster, cheaper, better. Companies are just starting to integrate now. Database itself becomes the 'agency'. "Intentions-based design" – just go to the database.
5. Transform – theoretical - merging agencies due to integration – reorganization on the back end.

Solutions:
1. PKI – Public Key Infrastructure – symmetric key, asymmetric (public/private) cryptography. If you know formula – single key formula – incrypt/decrypt – but don't know if someone has 'cracked' it. How can we deal with people securely without first giving them the 'code' first. Two formulas -public and private – anything encrypted with one key can only be decrypted with the other. Simply authenticate identity. SSL (secure sockets layer) – amazon – first tcp/ip – then html – then ssl.

How do you know that it is Amazon in the first place (how to initially get the public key)? PGP (pretty good privacy) – 'web of trust' – history of relationship (Phil Zimmerman) – keychain. Trusted 3rd Party (Santa Claus) – signature. i.e. certificate authority (CA) is given private key by everyone – they sign all data (name, key, etc) – then amazon presents to customer and decrypts CA's encrypted data – therefore identity is confirmed. Today and future – all politics is local (Tip O'Neill) – all identity is local. Relationships are context-driven.

Core ID – Central National Authority – link all IDs back to this Core ID – in order to use the same 'certificate' for all transactions. What is the underlying problem statement? Must ensure there is only one Core ID per person.

Loss of autonomy with Core ID – privacy and liberty problem. So alternative system is one of 'various realms of identity' – innocent citizen – have identity as a employee, as a citizen, as a consumer, as a parent, etc.

Name is only part of identity. English Common Law – you can change your name – as long as you are not trying to deceive. So who defines you? Yourself? Multinational corp? Gov't? This is the Liberty Alliance System.

Application to Our System
How should identity be managed in our system?
1. Do these users know each other in physical world? If no: strict ID is more important. If yes: more important to be anonymous.
2. ID should be configurable to sub-communities (alias/pseudonym)
3. Site design must track the underlying community norms w/ respect to ID.
4. Gradient of identities – flexible IDs (1.chatroom – 2.tv – 3.newspapers – 4.bank) – depends on the topic and you input (like, if you criticize someone)
      a) users should be able to select levels of ID, unless
      b) community requires certain level for particular action
sample levels: a) anonymous
             b) anon., unless accuse, then ID
             c) initial ID, then anon./pseudonym
             d) total ID

What is the meaning of ID in these contexts?

What about mimesis, simulacra, doppelganger, clones – are these are exceptions?

Reminders:
Tell Dan to send out website – public/private key.
Tell Dan to send link to Liberty Alliance Technical.
Tell Dan to send article by Dan G. on 'opting out'.