**Administrative**

- This week’s office hours for Dr. Neuman are today from 12:30 to 1:00 PM (or as late as necessary if students are waiting to see me). (No Friday office hours since Friday’s lab lecture is by Dr. Ryutov)
- Jonathan Kelly’s office hours until Mid-term are Friday from 1 PM to 2 PM, and Tuesday 1 PM-2 PM in SAL 1-10a.
- First assignment returned today.
- Mid-term in class next week.

---

**Passport v Liberty Alliance**

- Two versions of Passport
  - Current deployed version has lots of weaknesses and is centralized
  - Version under development is “federated” and based on Kerberos Liberty Alliance
  - Loosely federated with framework to describe authentication provided by others.

---

**Passport v1**

- Goal is single sign on
- Implemented via redirections

![Diagram](image)


---

**Federated Passport**

- Announced September 2001
- Multiple registrars
  - E.g. ISPs register own users
- Kerberos credentials
  - Embedded authorization data to pass other info to merchants.
- Federated Passport is predominantly vaporware today, but .net authentication may be where their federated model went.

---

**Liberty Alliance**

- Answer to MS federated Passport
- Design criteria was most of the issues addressed by Federated Passport, i.e. no central authority.
- Got off to slow start, but to date has produced more than passport has.
- Use SAML (Security Association Markup Language) to describe trust across authorities, and what assertions means from particular authorities.
- These are hard problems, and comes to the core of what has kept PKI from being as dominant as originally envisioned.
- Phased approach: Single sign on, Web service, Federated Services Infrastructure.
Review for Mid-term

- Cryptography
  - Basic building blocks
  - Conventional
    - DES, AES, others
  - Public key
    - RSA
  - Hash Functions
  - Modes of operation
    - Stream vs. Block

Review for Mid-term

- Key Management
  - Pairwise key management
  - Key storage
  - Key generation
  - Group key management
  - Public key management
  - Certification

Review for Mid-term

- Authentication: Know, Have, About you
  - Unix passwords
  - Kerberos and NS
  - Public Key
  - Single Sign On
  - Applications and how they do it
  - Weaknesses