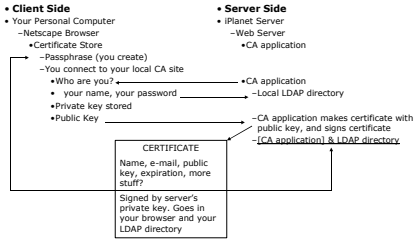
Dartmouth College — Mellon PKI

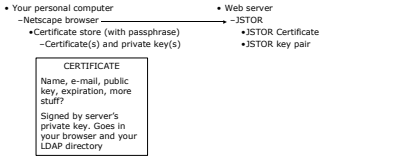
- NIH/HEBCA pilot participation
- Infrastructure Setup (following HEPKI PKI-lite)
- Web Resource Access (JSTOR)/"DRM"
- S/MIME Pilot
- Workflow Investigation/ Attribute Certificates
- Trusted Third Party Infrastructure - "Armor the pipe"
- End User Study Design
- Website Development

• Larry.Levine@dartmouth.edu

Enrolling in the local CA



Authenticate to a web site



— Next —

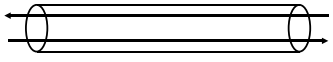
Normal plain old anonymous SSL with no personal certificates

— or —

SSL with personal certificates

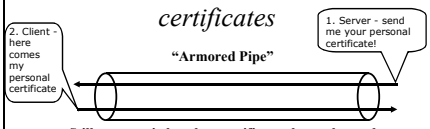
Normal plain old anonymous SSL with no personal certificates

"Armored Pipe"



Symmetric Key from server used to encrypt information

*Client-side SSL **with** personal certificates*

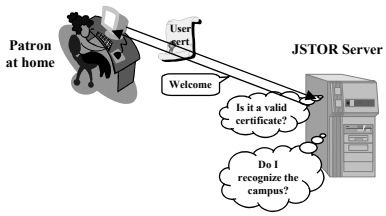


Still symmetric key, but certificate also exchanged

Certificate may be sent automatically or you may be prompted for which certificate and passphrase to use. (Or, perhaps a dongle certificate.)

Your certificate is received along with 'stuff' signed by your private key. Your signature is checked. JSTOR looks at your certificate [chain] and makes a Go/NoGo decision, may record info, ask you questions, etc.

The basic conversation



A few PKI questions

- How many key pairs and certs? Sign, encrypt, authenticate, etc?
- Where store private keys?
- Revoke? Expire?
- What's in a certificate?
- How grant a certificate and keys?
- Where put/store a certificate and keys?