The MIT CA Experience

Jeffrey I. Schiller

Massachusetts Institute of Technology

Introduction

- MIT Built its PKI in 1996
  - In the belief PKI would “take over the world”
    - I'm still waiting…
  - We have about 40,000 “live” certificates
  - Over 1.6 Million issued since 1996
  - Originally were v1 certs, now v3 certs
- Major Application: Web Authentication

Buy vs. Build

- Vendor solutions were (are) complex and expensive
- Notion of charge per certificate
  - Non trivial charge per certificate
- Build: Fixed cost of software development
  - Not a function of number of certificates
  - Flexibility to have many certificates per user

Technology Requirements

- Easy to Use
- Cost Effective
- Incrementally Deployable

Easy to Use

- We are slaves to the Browser Vendors
  - We support Netscape, Mozilla, IE and Safari
  - We work around the largest problems
- Biggest Problem: Exporting Certificate and associated keys to import into another system
  - Work Around: Obtain multiple certificates
  - Works because we only do Web authentication

Cost Effective

- Home grown software doesn't have a cost per certificate
- "Standard" Support costs that you expect from any software product
  - Actually, not that bad, we issue ~ 1,000 new certificates (freshman) each summer with ~ 10-20 problems

Incremental Deployment

- Not all applications at MIT use Certificates yet
  - But we encourage their use
- 99.9% of Students have certificates
- 66% of Faculty and Staff have certificates
  - This number will go up as applications they must use are converted (from paper!)

MIT CA Implementation

- Up to version 3
- First two versions based on Java and Cryptix toolkit
  - Version 1: servlet
  - Version 2: jsp
- Version 3 about to be deployed
  - Based on Python front end to openssl
    - Does not “fork” scalable implementation

Registration Procedure

- Certificates obtained by authenticating to CA website with Kerberos name, password and MIT ID Number
- Kerberos name is issued via a "Coupon" with six word secret
  - Only valid for initial account creation and can only be used once
  - Coupon mailed to students during the Summer
  - Website permits authorized staff to create duplicate PDF file for students who lose it

Tips

- Revocation is rarely if ever asked for
  - We do not encode authorization into certificates
- Most people don't know when they are compromised, so they don't request revocation
- May have to deal with this soon

Certificate Lifetimes

- All certificates issued prior to June expire July 31st
- In mid June we advance the “dead date” further 1 year
- Certificates issued to freshman from off-campus computers expire on September 1st
  - So they don't leave them on their parent's computer

Services Offered

- Web Authentication
  - Student Registration
  - Employee HR "Self Service"
    - Health care enrollment etc.
  - On-line purchasing
    - Partners accept our certificates
  - Many others

What we do not have

- A Certificate Practice Statement
- A Certificate Policy Statement
- In “practice” no one in the “real world” (read: not the government) cares
- Biggest issue with outside vendors is helping them get infrastructure setup
- It is always more secure then issuing names and passwords

Future

- S/MIME Support
  - Challenge due to multiple certificates and key escrow issues
  - Most S/MIME implementations store encrypted messages in the original encryption key
    - This is probably a bad idea
  - Encrypted mail is more important to us then signed mail