UW Certificate Services Go Commercial

This information is adapted from "UW Cert $ervice Goes Commercial (!$!)" presented at the June 30, 2011, UW Web Services Discussion Group meeting.

UW PKI History 1

- C&C used to facilitate cert purchases for UW
    - stopped many years ago as market fragmented
    - so depts have been on their own in commercial cert marketplace ...
- PKI: still waiting for Elvis moment ...

UW PKI History 2

- 2002: PKI Planning Project
- Many possible services:
    - secure email
    - document signing/encryption/archiving
    - code signing
    - user authentication (web, VPN, etc)
    - (Windows variations of all the above)
    - SSL certs

UW Services CA

- X.509 certs for SSL/TLS
    - web (HTTP) servers
    - other servers: LDAP, IMAP/POP, ...
    - (HTTP) clients
    - UW-developed server, "standalone" root
    - started operations mid-2003
    - 8,000+ certs issued; 1,200 current
    - relies on UW DNS for hostname ownership, so issuance can be instantaneous

UW Services CA Issues 1

- Supportable?
    - users get "untrusted site" warnings
    - browser root install can be pain, changes all the time
    - hasn't been a problem for UW-IT helpdesk;some departments have had trouble

UW Services CA Issues 2

- Not usable for sites with many (non-UW) users
- Not usable for non-UW-named sites
- Risk in local code base ...
- Client certs on Windows ...

InCommon Certificate Service

- extension of InCommon trust services
- make a deal with a Commercial CA to get flat rate on unlimited certs for HE customers
- following lead of European HE, who have been doing this since 2005 or so
- rolled out summer 2010
- 100+ current customers

InCommon Cert Services

- SSL certs, client and server
    - these are the obvious draw, and most used today
- Extended Validation (EV) certs
- Code-signing certs
- "Personal" certs

UW Commercial Cert Use?

- Exact numbers hard to get, but UW units spend at least $75K / year on commercial certs
- InCommon price for UW-sized institution is $15K / year
- So, what's not to like...?

Like

- UW-IT completed purchase of InC service a couple of weeks ago
- will fold into standard UW-IT service bundle (i.e., no extra charge to depts)
- SSL certs for all UW domains and subdomains

- *.washington.edu, *.uw.edu, *.uwb.edu, *.uwmedicine.org, etc
- also non-UW domains if UW ownership can be shown

InCommon Cert Service Benefits

- $ave money
- reduce SSL cert purchasing hassle
- more certs for more sites
  - sites where current cost is a burden
  - non-UW-domain sites
- better tracking / notification ?

It's a Free Lunch!

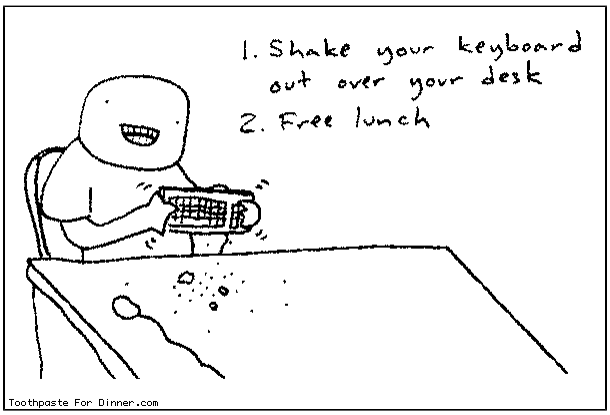

Image source: http://www.toothpastefordinner.com/

Risks

- InCommon + vendor relationship could go bad
  - 3-year contract might not be renewed
- Vendor can have technical service problems, eg service outages / delays
- Vendor can have fundamental problems

The Recent RA Compromise

- On March 15th 2011, a Comodo affiliate RA was compromised...

Post-compromise ...

- Comodo now performs human review of all cert requests, so issuance has gone from seconds to about 24 hours
- Would OS/browser vendors ever remove a CA?

Integration

- Comodo provides classic web UI for cert management
  - site admins delegate to dept admins ...
- ... but UW CA gets value from relying on UW DNS for name ownership
- Comodo also provides a web service interface
- So current UW-IT plan is to make InCommon an option under existing UW Services CA web UI

Transition?

- Two CAs?
  - yes, for a while, maybe forever
- some UW servers require UWSCA-issued client certs, would have to change to accept InC/Comodo
- UW CA will probably always have faster turnaround
- UW-IT will provide support info about which to choose

Beyond SSL certs?

- Code-signing certs useful in some cases, probably handled specially
- EV certs probably useful for some key websites (weblogin, www.uw.edu ...)

Personal Certs?

- personal certs remain appealing for user authentication, email, signing/encryption, etc
- but barriers to use from 2002 haven't changed much; InC/Comodo service doesn't help much with those

- some campuses are working on rolling them out ...

When when when?

- Working on integration now, no firm date for rollout
- Certs expiring in June? Get 'em the old-fashioned way
- Certs expiring in a few weeks? Let us know (iam-support@uw.edu) and we'll see about getting them issued