Client Certificate Deployment strategies

Presentation by Joe St. Sauver (Internet2 and University of Oregon), focused on client cert deployment models, but many of these points will resonate with, and be applicable to, other multi-factor approaches. Original can be found at:
http://pages.uoregon.edu/joe/client-cert-models/

Some key points (slide titles) from this pdf of a slide presentation at the Internet2 Joint Techs meeting in January 2012:

- The InCommon Certificate Program
- Client Certificate Deployment
- Why haven't PKI certs thrived the same way SSL certificates have?
    - It Isn't Simply That PKI Is "New"
    - Economics? Are Client Certs Too Expensive?
        - But In Some Cases, Client Certs Are "Free"
    - Is Usability Actually The Problem?
        - But Things Have Come A Long Way, Usability-Wise
    - Or Is The Problem That Other Solutions Have Usurped PKI's Market Niche(s)?
- A Humorous Comment With An Underlying Grain of Truth? The PKI DeLorean* Hypothesis
  "[M]aybe the possible future in which everything is PKI-enabled and digital certificates are ubiquitous is so horrendous that it actually sent ripples of bad luck back through time that sabotaged the development and deployment of PKI technology. Some things actually seem to make a lot of sense from this point of view."
  "Why PKI Failed," Luther Martin, 29 October 2009,
  http://superconductor.voltage.com/2009/10/why-pki-failed.html [a blog about security, cryptography and usability]
- "Fixing PKI" – A Cottage Industry of Its Own
- So Today We're Going To Focus On Deployment Models, Not On Use Cases
- Client Cert Deployment Scale: Test, Departmental, Site-Wide, edu-Wide?
    - Small Deployments? ==> Targeted Benefits
    - Larger Deployments? ==> Broad Acceptance
- A Standardized Higher-Ed-Wide ID Card? (I.e. Smart card)
- Two Models For Cert Deployment Rigor: A. "fairly casual" or B. "much more rigorous"
- We **COULD** Even Go Beyond Model B... (U.S. Govt. CAC/PIV)
- But Let's NOT Go Overboard In Higher Ed
- So what might be a "doable" target cost per user per year?
    - How about a Target Cost: $1/user/month (inclusive of all costs)?
    - Discounts for Hard Tokens/Smart Card?
- "But Do We Even Really Need To Deploy Hard Tokens or Smart Cards?"
    - Users Don't "Map" To A Single Computer
    - "Why Not Just Issue New Credentials To Each Computer A User Might Work With?"
    - Hard Tokens/Smart Cards Have Advantages
    - Getting An Institutional ID (or Door Key)
    - Using An Institutional ID (or Door Key)
- CAC/PIV Is A "Proof By Example" That Smart Cards Are Usable By "Mere Mortal" End-Users
- Granted, Smart Cards/Hard Tokens Aren't Perfect
- How Easy Would Doing Hard Tokens/Smart Cards Be From the Point of View of Card Admins?
- A Sometimes Overlooked Challenge To Deployment of PKI at Scale: Directories
    - Some Directory Complications
    - How About PGP-Style Keyservers for S/MIME?
- One Closing Caution: Client Certs Are Now Being Targeted By Malware

File	Modified
PDF File ClientCertDeploymentModels.pdf Client Certificate Deployment Models, and Hardware Tokens/Smart Cards	Feb 17, 2013 by Michael Grady (unicon.net)