



Cornell Information Technologies
ADVANCED TECHNOLOGY & ARCHITECTURES

Using PDFs to Exchange Signed, Encrypted Data

Ron DiNapoli

Cornell University, CIT/ATA

5th Annual PKI R&D Workshop



Cornell Information Technologies
ADVANCED TECHNOLOGY & ARCHITECTURES

Who Am I?

- ◆ Worked with Kerberos/Central Authentication 1999-2004 at Cornell.
- ◆ Have attended various PKI related events since 2000 (CREN, NIST, Dartmouth).
- ◆ Began working for a small group at Cornell looking at advanced technologies in 2005.
- ◆ Looking at PKI usability/feasibility with respect to the Cornell environment since April 2005.



Cornell Information Technologies
ADVANCED TECHNOLOGY & ARCHITECTURES

Agenda

- ◆ Apologize to those expecting answers
 - *My goal is to raise a question*
- ◆ What problem am I trying to address?
- ◆ Make some assumptions about problem
- ◆ Ask some questions about problem
- ◆ Test premise that there are no stupid questions
- ◆ Q & ?



Cornell Information Technologies
ADVANCED TECHNOLOGY & ARCHITECTURES

PROBLEM:

A Recurring Theme

- ◆ **User Experience with PKI is Bad!**
 - Why Johnny Can't Encrypt (1999)
 - Alma Whitten's talk on custom mail client at 2nd annual PKI R&D Workshop (2003)
 - Dartmouth Summit: User Experience big reason for lack of deployment (2004)
 - PKI '05 User Experience BOF



Cornell Information Technologies
ADVANCED TECHNOLOGY & ARCHITECTURES

What is the Solution?

- ◆ Could it be as simple as “Fluffy”?
 - Does PKI need a mascot? :-)
- ◆ Seriously...
- ◆ Early 90s: Kerberos had KClient
 - Common end user interface
 - Made Kerberos easier to use on more platforms for more people
- ◆ Can we learn from the past?



Cornell Information Technologies
ADVANCED TECHNOLOGY & ARCHITECTURES

Where is My Focus?

- ◆ Focus on “commodity” uses where we might expect a large number of “novice” users to need to understand PKI
 - Web Authentication
 - Signed/Encrypted Email
 - OS Level Login/Access
 - Custom (in-house) applications



Analyzing the Problem

◆ Apologies to mathematicians...

“End User Experience Support Expression”

- $(e + w + 2) * p$

- e: # of email clients (with PKI support)

- w: # of web browsers (with PKI support)

- p: number of operating systems (platforms)

- “2” for 1 OS Level Login experience and 1 experience for custom applications



Cornell Information Technologies
ADVANCED TECHNOLOGY & ARCHITECTURES

How Do We Deal with this Problem?

- ◆ Start by sorting the uses into two “everyday experiences”
- ◆ Authentication
 - *OS Level Login, Web Authentication, Custom Applications*
- ◆ Encryption/Verification
 - *Signed/Encrypted email, Custom Applications*



Cornell Information Technologies
ADVANCED TECHNOLOGY & ARCHITECTURES

A Possible Solution

- ◆ Authentication and Encryption/Verification uses are (clearly) different experiences
- ◆ Can we unify these experiences across applications on each supported platform?
 - One authentication experience per OS
 - One encryption/verification experience per OS



Cornell Information Technologies
ADVANCED TECHNOLOGY & ARCHITECTURES

Benefits of Unification

- ◆ Remember the expression:

$$(e + w + 2) * p$$

- ◆ With Unification, this becomes:

$$2 * p$$

- One authentication experience
- One encryption/verification experience
- Multiplied by the number of supported platforms



Cornell Information Technologies
ADVANCED TECHNOLOGY & ARCHITECTURES

Unified Authentication?

- ◆ Can the authentication experience be unified on each platform?
 - Not perfect, but examples of consolidation of PKI related operations at the OS level:
 - Windows–CAPI
 - Mac OS X–Keychain/Certificate Services
 - UNIX/Linux–M.U.S.C.L.E?
- ◆ But since this is a *digital signatures* panel we'll focus on...



Cornell Information Technologies
ADVANCED TECHNOLOGY & ARCHITECTURES



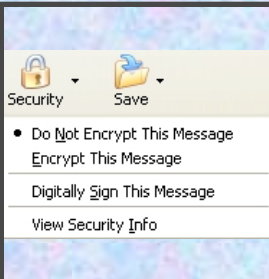
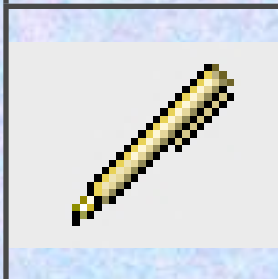


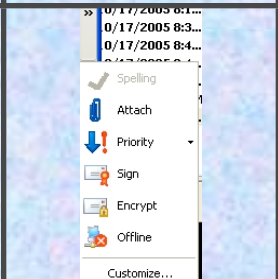
Unified Encryption/ Verification?

- ◆ More problems here...
- ◆ Different experiences across applications on the *same* platform
 - Eudora/Outlook/Mail.app/Thunderbird do it differently
 - Safari/Firefox/IE
 - Custom applications



Cornell Information Technologies
ADVANCED TECHNOLOGY & ARCHITECTURES

Examples of Some Client Differences

- Apple Mail's verification of sender's signature
 - Adobe's visual indicator of a document whose signature has been verified
 - Thunderbird's (Windows) user interface for encrypting a mail message
 - Apple Mail's interface for encrypting a mail message
 - Thunderbird's (Mac OS X) user interface for encrypting a mail message
 - Outlook Express' interface for encrypting a mail message
- Thunderbird's UI element indicating that the sender's signature has been verified

Can you match the picture to the explanation?



Cornell Information Technologies
ADVANCED TECHNOLOGY & ARCHITECTURES

Can PDFs Help with Unification?

- ◆ Let's look at in the context of encryption/verification...
- ◆ PDFs can be signed/encrypted/verified
- ◆ Infrastructure is *already deployed* to majority of end user systems
- ◆ UI elements are reasonably the same on all platforms
- ◆ End users are likely already familiar with PDF/reader technology
- ◆ Can PDFs be used for all of our encryption/verification needs? If it could...



Cornell Information Technologies
ADVANCED TECHNOLOGY & ARCHITECTURES

Can PDFs Help with Unification?

- ◆ Since PDF technology is reasonably the same across platforms, our “unified” expression:

$$2 * p$$

- ◆ Actually becomes:

$$p + 1$$

- Where “p” is the number of os-specific Authentication experiences we need to educate users on and the “1” represents educating users on PDF technology.
- Much better than $(e + w + 2) * p$



Cornell Information Technologies
ADVANCED TECHNOLOGY & ARCHITECTURES

But Would it Work?

- ◆ Back to the million dollar question...
- ◆ Can PDF technology replace existing encryption/verification technology in commercial and custom applications?



Two Types of Data

- ◆ **Visual or Static**

Equivalent to the concept of sending
“paper” to each other

- ◆ **“Live” or Dynamic**

Equivalent to the notion of sending “files” to
each other

Recipient may wish to modify and send to
someone else



Cornell Information Technologies
ADVANCED TECHNOLOGY & ARCHITECTURES

Signing/Encrypting Visual/Static Data

- ◆ This works today
- ◆ Use any PKCS#11 token
- ◆ Use a certificate in software store
- ◆ You can encrypt based on a user defined password or the Adobe Policy Server

Policy Server gives you more control over who can see the data and what they can do with it



Cornell Information Technologies
ADVANCED TECHNOLOGY & ARCHITECTURES

Signing/Encrypting Live/Dynamic Data

- ◆ **Some support in Acrobat/Reader**
 - Form data in PDFs
- ◆ **Less elegant solutions**
 - Attach files directly to PDF container
 - Adobe's PDF To Text Conversion (web site)
 - Search the Internet: "Convert From PDF"
 - In each case: Lose signing history!



Cornell Information Technologies
ADVANCED TECHNOLOGY & ARCHITECTURES

Conceptually, Where Does This Work?

- ◆ This concept works for applications such as:
 - Web Browser file level uploads/downloads
 - Mail Clients
 - Just need to be able to handle attachments
 - Great given the lack of unified user experience for S/MIME
 - Any other application that assumes data to transfer is in a dedicated file



Conceptually, Where Doesn't This Work?

- ◆ Applications which do not use files to transfer data.
- ◆ Can PDF technology be built into custom applications such that separate files are not needed?
 - Not really
 - Adobe has an “SDK”, but assumes Java/Servlet/HTTP app
 - No way to access hardware token on local machine
 - Still file based



Cornell Information Technologies
ADVANCED TECHNOLOGY & ARCHITECTURES

Demonstration

**Signing a PDF
(Hardware Token)**



Cornell Information Technologies
ADVANCED TECHNOLOGY & ARCHITECTURES

So, Does it Work?

- ◆ Based on issues with dynamic data, it appears to fall short.
- ◆ Is there hope for tomorrow?
 - Technology is already deployed
 - Adobe appears to be open to suggestions!
 - Minimally: Is this concept a good blueprint for the “real” solution?



Cornell Information Technologies
ADVANCED TECHNOLOGY & ARCHITECTURES

Demonstration

Encrypting a PDF
(Policy Server)



Cornell Information Technologies
ADVANCED TECHNOLOGY & ARCHITECTURES

Q & ?

Any Questions?