

Adoption of PKI

Where are we, where should we be, what's holding us back, and where do we want to go?

And: what about authentication vs. authorization?

Rich Guida

What are the framing issues?

- What applications need authentication, e-signatures, or confidentiality?
- What determines the degree of need?
- What is the nature of the population of users an application services?
- What is the span of control of the PKI intended to service that application?
- Do you justify a PKI based on Return on Investment or something else?
- Does the PKI handle user authorization or just authentication?

Where are we?

- PKI is being broadly used for SSL server-side authentication
 - Whether it provides all of the security one might like or not
- PKI is seeing growing acceptance within enterprises as a tool for user authentication, e-signatures, and confidentiality
 - Many examples, government and private sector
- PKI is starting to be used between enterprises and in IPSEC
- But PKI is NOT being used globally by consumers
 - With some notable exceptions (e.g., ScotiaBank)
- And PKI is also not being used broadly for user authorization
 - Attribute certificates still a “work in progress”

Where should we be?

- Using PKI broadly for authentication, and ultimately authorization
- Integrating PKI into the network and enterprise directory services, so it can benefit from them
- Providing a common look and feel at the application layer for certificate use
- Making the use of certificates seamless and “reasonably” invisible to the average user

What's really holding us back?

- Lack of applications that use certificates
- The race to be “second”
- Lack of common semantics (e.g., in certificate policies)
- Organizational politics (e.g., Intra-organizational and inter-organizational parochialism, NIH syndrome, namespace control, lawyers)
- Dealing with legacy application entanglements
- Lack of an ability to show ROI (a chimera)
- And least of all – the technology

Where do we want to go?

- Depends a lot on your perspective
- Some want to see identity-based PKI burgeon for intra-enterprise use first, then inter-enterprise
- Others want to see identity-based PKI burgeon for dealing with consumers or the public
- Others would like PKI to focus on authorization rather than authentication
- Still others think we should use some other technology entirely
 - But what? Passwords? Biometrics? Each has its own set of problems...

Authentication vs. Authorization

- If an application needs to do one, it probably also needs to do the other
 - Or needs to trust another application (or the network operating system) which has done the other
- Can do both simultaneously, or separately
 - “Should I separate variables before solving this PDE?”
 - (Normally – yes, especially if the PDE is Navier-Stokes!)

Why do Separately?

- Intuitively consistent with processes we are all familiar with
- Required by some (perhaps most) regulations (e.g., FDA 21 CFR Part 11, e-records, and e-signatures)
- Allows PKI to do one while some other process does the other (thus, supports legacy applications that use ACLs)
- Sometimes identity is important separate from authorization (or identity is sufficient by itself – such as patient access to his/her records under HIPAA)

Examples

- Passport
 - To get one, have to prove who you are (don't even have to indicate "why") – but if you want to use it, may need a visa (authorization to visit foreign country)
- Driver's license
 - To get one, had to prove who you are, not just that you can drive a car, and license provides evidence of identity as well as authorization to do something – drive a vehicle
- Getting a credit card
 - To get the card, had to provide evidence of who you are and ability to pay your debts (former needed to establish latter)
 - Arguably you should be asked to provide stronger evidence than credit card companies require (to combat identity theft)
- Using a credit card
 - Some merchants accept card alone for purchase (so it is like an authorization token), but increasingly you have to produce separate identity ID because of problem with fraudulent purchases

Example: Johnson & Johnson PKI

- Directory-centric
 - Enterprise directory serves as authoritative source
 - Certificate contents come solely from directory
- Two identity certificates (signature, encryption), plus role/group certificates
- Hardware token preference (USB iKey2032) but also support software tokens
- In first phase of deployment (about 500 certificates issued), testing underway
- Second phase (full production) later this year
 - Goal is certs for almost all J&J employees plus, where necessary, customers and business partners
 - Expect total number ultimately to be >>100,000
 - Willing to accept non J&J certs through cross-certification or trust list model

J&J PKI – Key Uses

- Remote authentication with hardware token only (VPN using Nortel Contivity client)
- Authentication to enterprise software (e.g., SAP, Siebel, Oracle)
- Digital signatures to comply with FDA 21 CFR Part 11 (authorization established separately)
- Encryption to comply with Healthcare Insurance Portability and Accountability Act
- Secure (signed/encrypted) e-mail for clinical trials, financial data, mergers/acquisitions, law department activities
- Automated Lab Instrumentation Management Systems (signatures and encryption)