



<http://www.carillon.ca/>

Public Key Infrastructure (And Fingerpuppets)

Dave Coombs

Director, PKI Standards and Policy

dcoombs@carillon.ca

ATA e-Business Forum – Oct 21, 2008

Outline

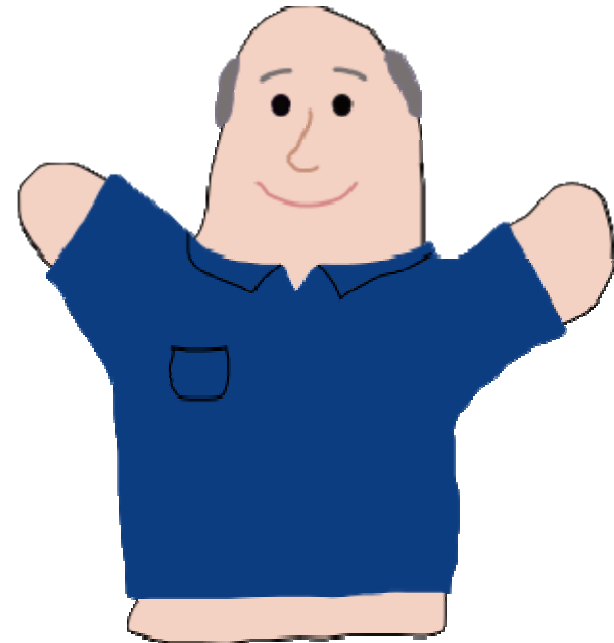
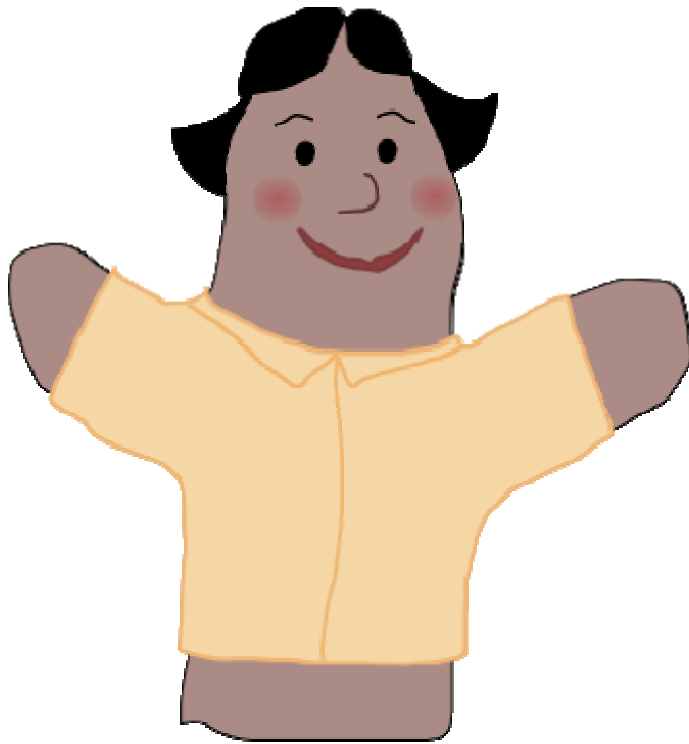
- Who's the skinny guy?
- Quick Survey
- What Makes Good Authentication?
- PKI Technical / Policy Components
- PKI Strengths / Weaknesses
- On an Aircraft

Quick Survey

- How many of you:
 - have some knowledge of PKI?
 - work at a company that's implemented PKI?
 - work at a company that's planning to implement PKI?
 - work at a company that's decided not to implement PKI?

Our Heroes

- Introducing Alice and Bob:



PKI is Really Good at:

- Authentication!
 - Technical component
 - Policy component
- If *both* done well
 - Identity assurance can be conveyed digitally
 - Comparable to photo-id and fingerprinting in real life

Typical Digital Authentication?

- Username/password
 - There are problems with passwords.



Old News about Passwords

- Key size, key quality
- “shovel”
 - breakable near instantly.
- “shovell”
 - breakable marginally less instantly.
- “shovelshovelshovelshovelshovel”
 - likely breakable in minutes?

128 bits?

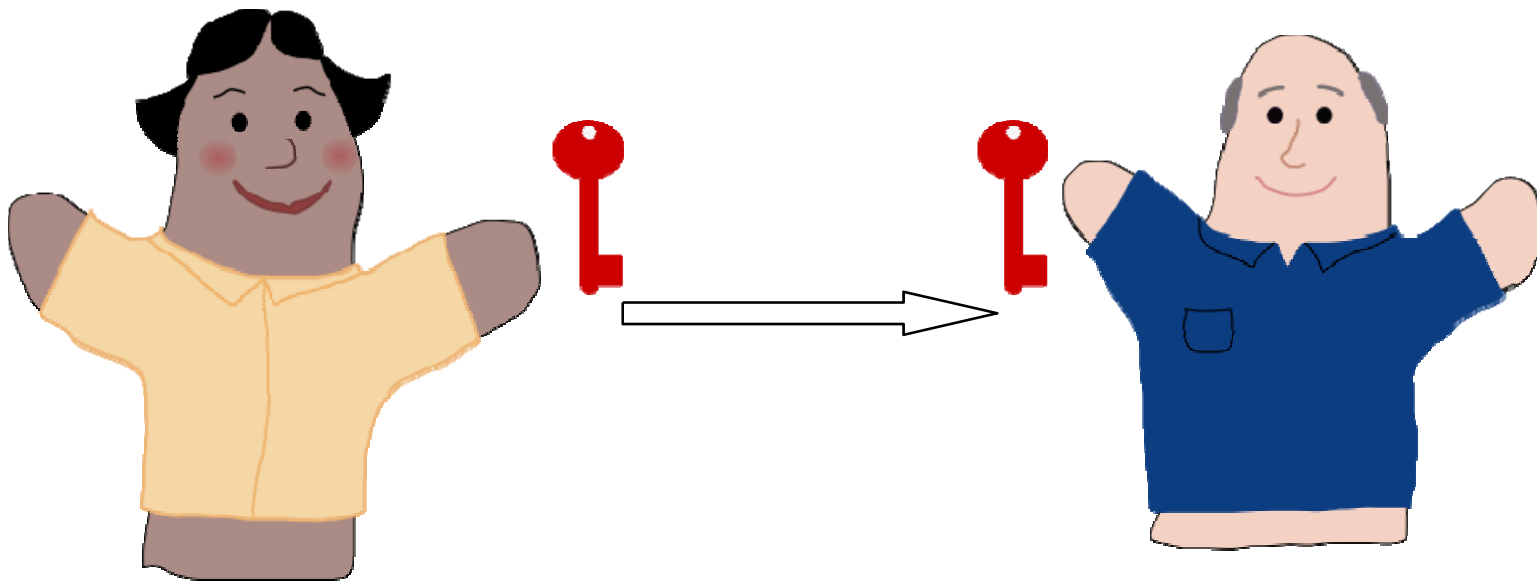
- Considered adequate for a shared key or a password
- $128/8 = 16$ characters
- “I enjoy carrots.”
 - English text has 2.3 bits worth of randomness per character (maybe even less)
 - Effective key strength is around 56 bits
 - Breakable in a matter of hours

A Good 128-bit Password

- “oVZ7tOdK0eoTW7P3VIBtyw==”
- Nobody in this room:
 - has a password like that
 - could remember it anyway

Back to Our Heroes

- Alice sends Bob a message
 - identifying herself with a password



- That password is either:
 - inferior, or written down somewhere

Introducing PKI

- PKI solves the password problem.
- *Makes* you have a good key.
- Makes protecting the key easy.

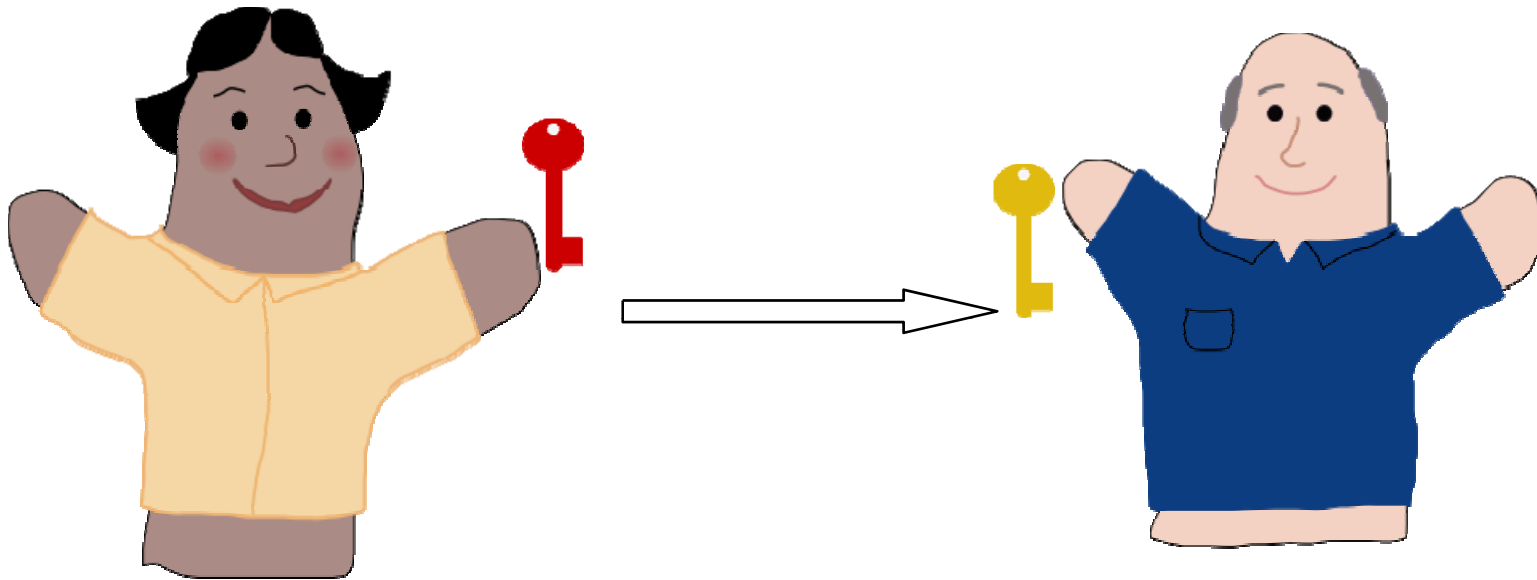
What the Insane Math Does

- Two related keys per person:
 - One public, one private
 - Given one, “hard” to find the other
 - Data processed with one can *only* be retrieved with the other

Key Quality

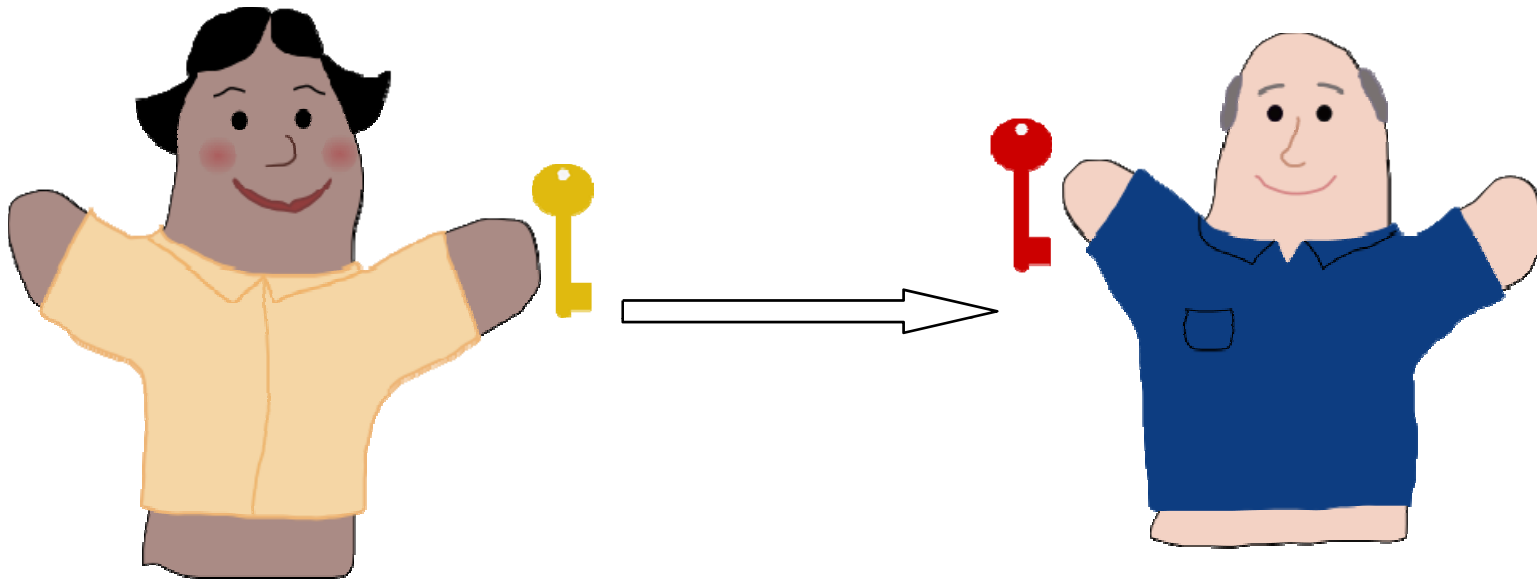
- Still important
- 2048-bit, randomly generated
- Private key stored in *one place only*
 - Software? Hardware?
- Public key distributed openly

Simplistic eg: Digital Signature



- Bob uses Alice's public key to verify her signature.
 - He then *knows* Alice's private key was what generated the signature.

Simplistic eg: Encryption



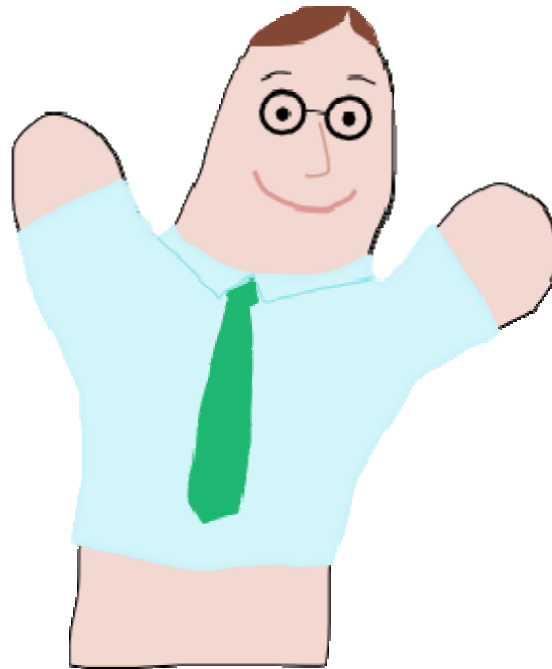
- Alice encrypts data with Bob's public key.
 - Then, *only* Bob's private key can decrypt it.

Real Life Intervenes

- Just as policy can't make a flawed technical solution perfect...
 - ...Good technology isn't enough on its own either.
- “Magic crypto dust”
- Policy is the other half of PKI...
 - ...The much more important half.

Certification Authorities

- This is Charlie:



- He runs a Certification Authority (CA).

Certification Authorities

- CAs issue Digital Certificates, once your identity has been validated to them.
 - “Trusted 3rd party”
 - “Electronic notarial service”
- Certificates contain:
 - A copy of the subject's Public Key
 - A digital signature from the CA
 - Pointer to CA's repository
 - Other stuff

Certificate Policy (CP)

- Describes *what* a CA must do to remain trustworthy. Mostly *non-technical*.
- Describes the conditions under which certificates are issued.
 - Type of identity checking.
 - Type of cryptography used.
 - Physical security controls at the CA.
 - Human security controls at the CA.
 - Allowable uses of certificate.
 - Audit procedure.

Audit Procedure?

- Audit procedure.
- CAs must be audited periodically
 - Usually every year
 - To make sure they comply with the CP
- For a relying party to trust a signature:
 - The CA's continued, audited operation, reinforces that trust. It gives it meaning.
 - Makes the certificate worth something.

This All Sounds Expensive

- Yes and no. There are tradeoffs.
 - Pay now vs pay later
 - Simple vs complex key management
 - Low vs high impact of key compromise
 - Rigorous vs ad hoc structure

How Secure is PKI?

- Key size is a factor.
- “Hard” problem: given public key, derive the other?
- As secure as the CP says.
 - Assurance level? Identity checking? Controls at the CA?
- As secure as the people involved.

PKI's Weaknesses

- Application support is .. variable.
 - Some apps interpret standards differently.
- Large up-front cost to start a CA.
 - Carillon usually recommends not to.
- Seen as overkill.
 - “Username/password good enough for me!”
- Seen as very specialized.
 - Good knowledge/support are rare... but getting better.

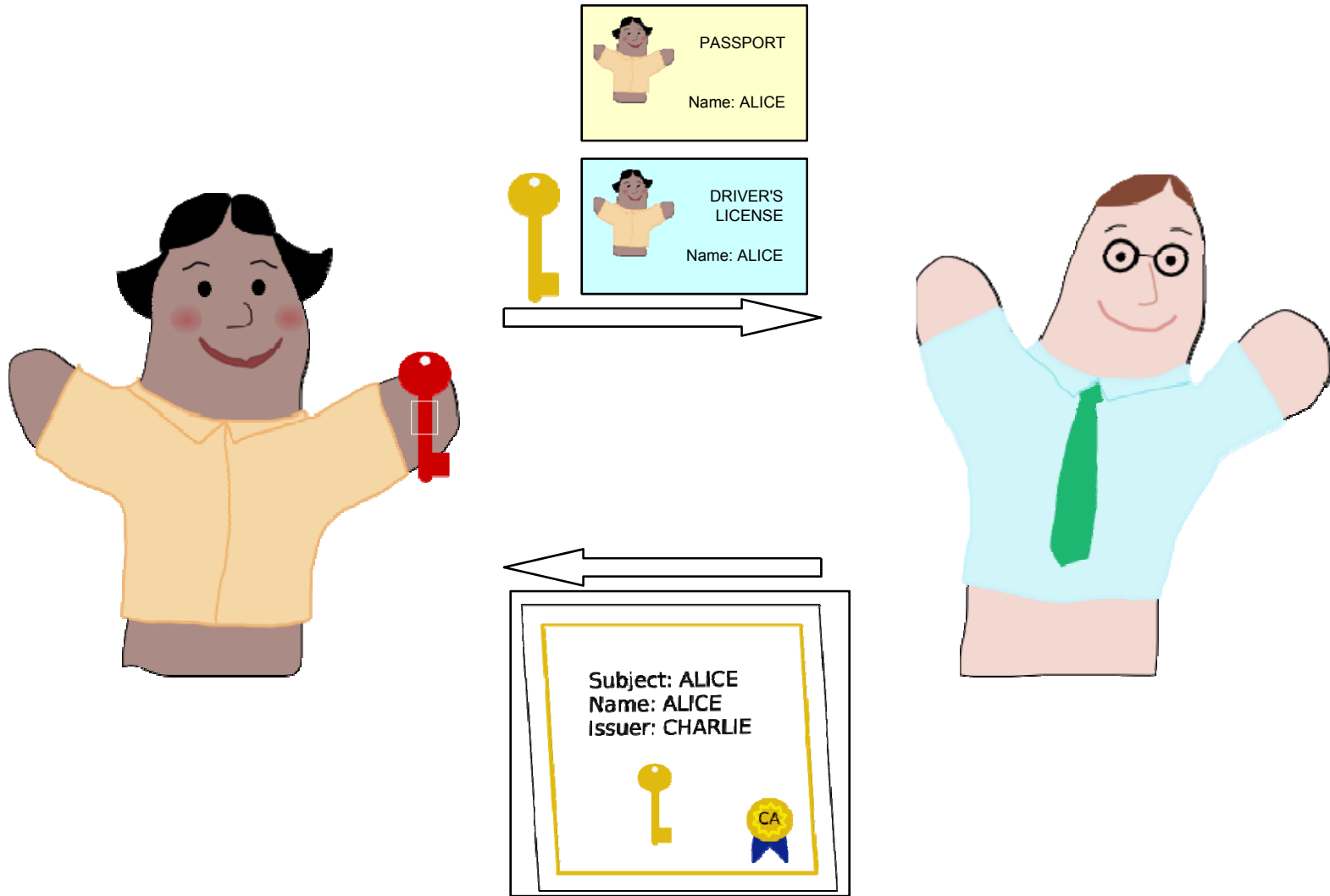
PKI's Strengths

- Collaborative, but independent
 - eg: TSCP
- Key management simplified
 - Rules clear, re-keying easy
 - Automatic renewals
 - Key compromise easy to deal with
- Stronger keys, usually held more securely
- Leverage investments in AD and/or other enterprise directory systems

PKI's Strengths

- Certificate support built into most OS's and web apps
- Secondary cost reductions
 - Digital signatures instead of crates of paper?
- Ties in naturally with smartcards/tokens
 - Multi-purpose smartcards/tokens?
- Promotes two-factor security
 - eg: smartcard + PIN

Registration



Certificate Issuance

- When Charlie issues Alice's certificate:
 - He's vouching for her identity.
 - He's putting his reputation as a CA at stake.
- Bob receives signed message from Alice:
 - Checks signature.
 - Checks validity of Alice's certificate.
 - Checks for revocation of Alice's certificate.
 - Checks Charlie's signature on Alice's certificate.

Revocation

- CA must publish a CRL
 - Certificate Revocation List
- Each certificate contains a pointer to the relevant CRL
- Bob's software retrieves Charlie's CRL
 - and checks for Alice's certificate.
 - If it's not there, the cert should be valid.

On an Aircraft

- Typical certificate lifetime is 3 years
- Coincides pretty nicely with heavy maintenance cycle
 - (by contrast, NIST suggests 1 year for a shared symmetric key)
- How keys are loaded onto aircraft avionics is an open question:
 - must satisfy regulatory requirements?
 - must provably be no key/cert tampering
 - permanently activated

On an Aircraft

- Aircraft move around.
 - Aren't always near a maintenance facility.
- Want to minimize maintenance!
 - Key compromise only affects one plane.
 - Fall back on insecure systems until fixed.
 - No one on board the plane can fix it.
 - No help-desk personnel like on a LAN.

For More Info

- ATA Digital Security Working Group
 - <http://ataebiz.org/>
- Fingerpuppet Theatre
 - <http://www.carillon.ca/library/howtos.php>
- Ask!

Thank you!

Questions?

<http://www.carillon.ca/>

dcoombs@carillon.ca