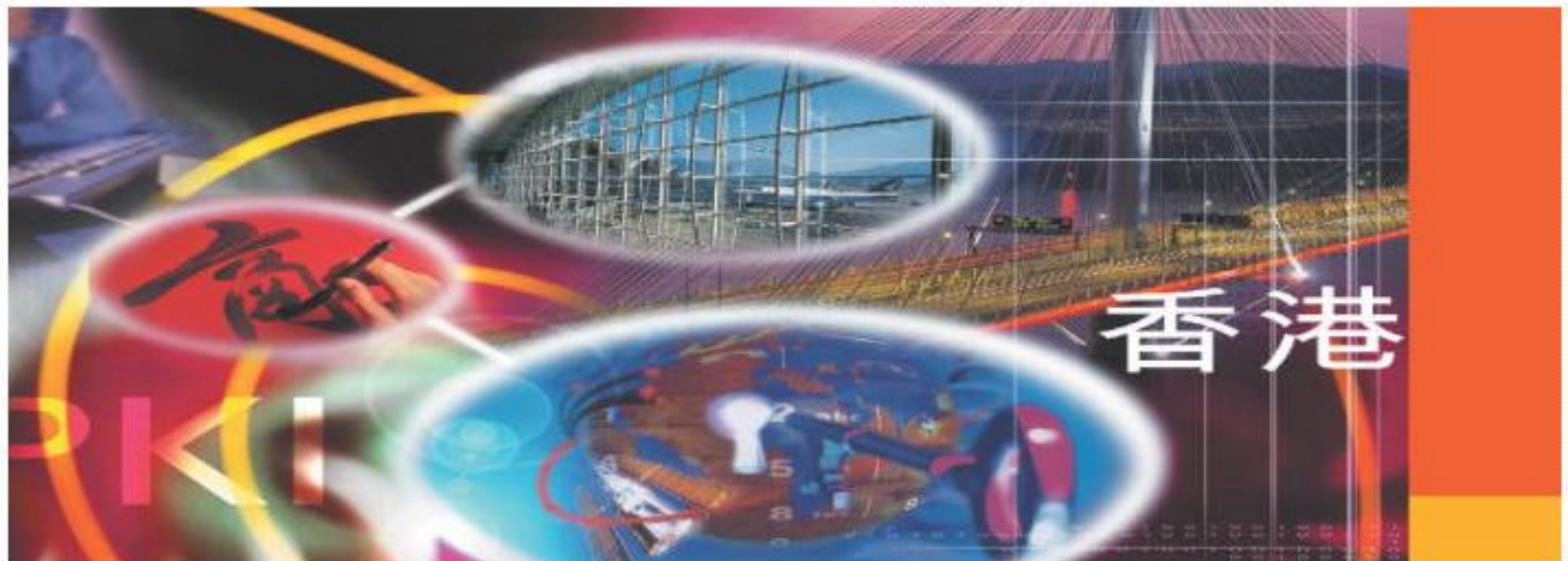


Truth in Advertising:
What PKI Can Really Deliver to Business

Mr. Thomas Parenty

President, Parenty Consulting, LLC





Truth in Advertising

What PKI Can Really Deliver to Business

Thomas Parenty

President, Parenty Consulting, LLC

Author, *Digital Defense: What You Should Know About Protecting Your Company's Assets*

Hong Kong PKI Forum

15 September 2003



Perspectives Based On ...

- 20 years of designing systems with encryption and other security technologies
- Not being a PKI vendor



PKI Trap

- Focus on public key encryption technology
- Without addressing
 - Business problems
 - System-wide security issues
 - External dependencies



Security Topics

- Establishing identity
- Keeping information confidential
- Accountability and integrity
- Controlling access

Knowing Who is Who in Cyberspace

Identifiers

E-mail address

Username

Digital Certificate

Authenticators

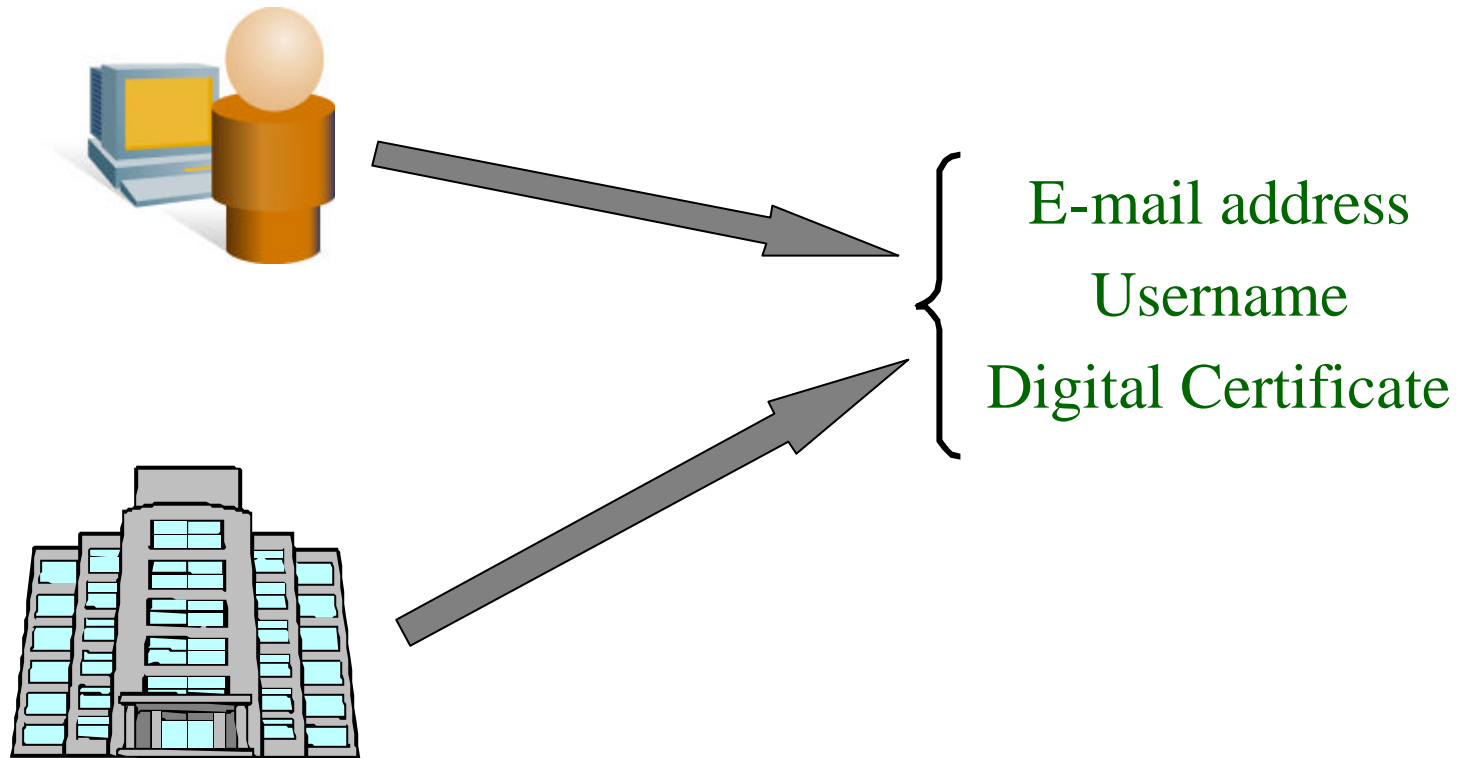
Passwords (know)

Tokens (have)

Biometrics (are)

Only Part of the Picture

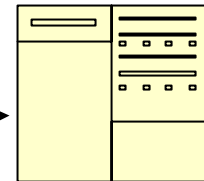
What's the Missing Piece?



Verified Digital Identity Creation

Confidentiality Threats

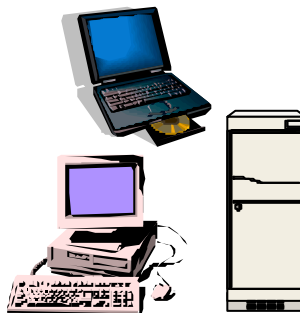
Network
Communications



Eavesdropper
“Wire”

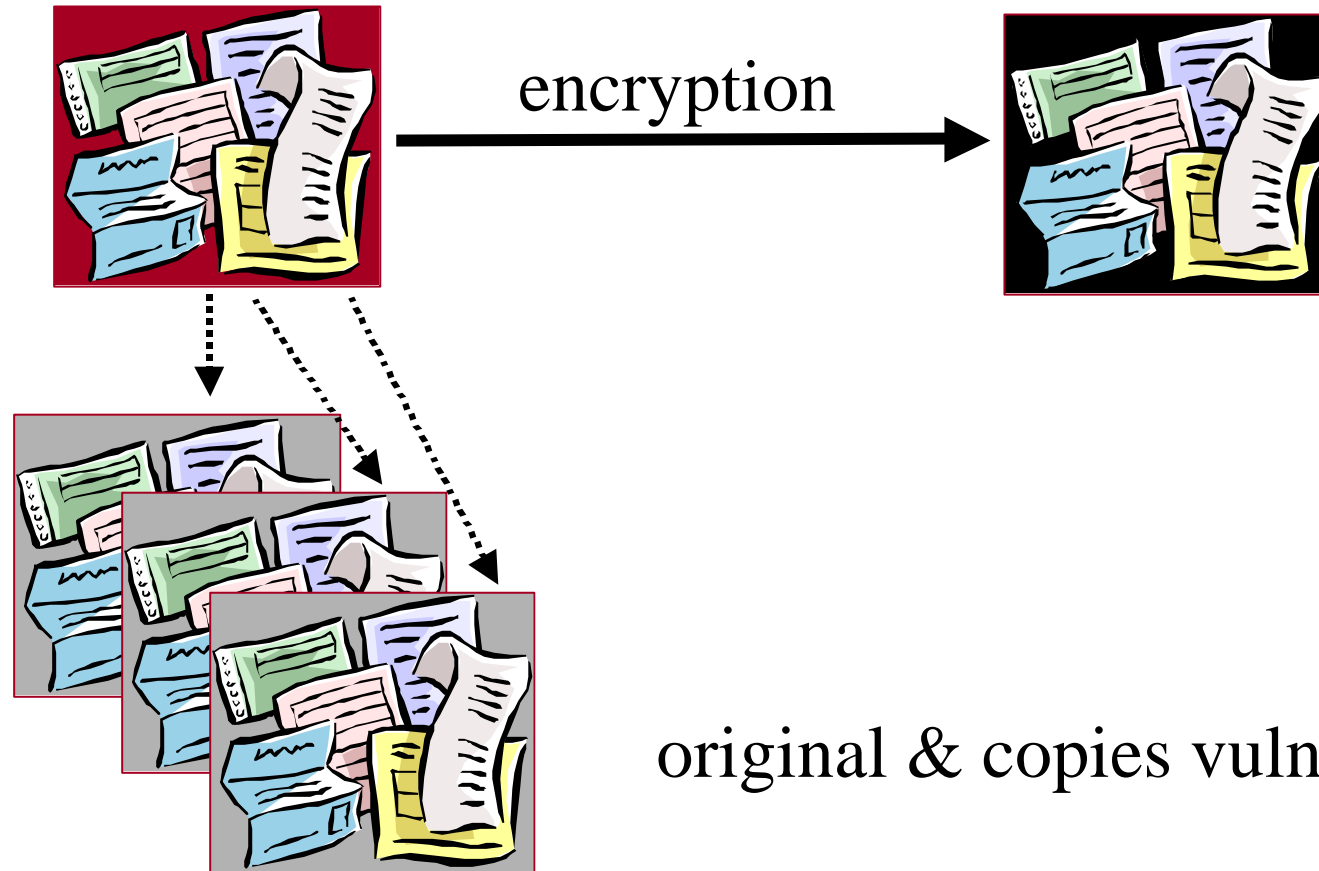
Intermediate Computer

Stored
Information



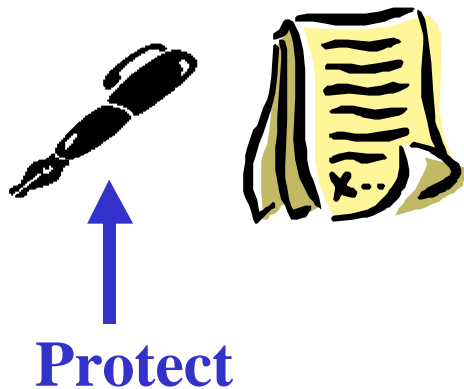
Physical Theft
Cyber Attack
Administrators

Protection more than Encryption

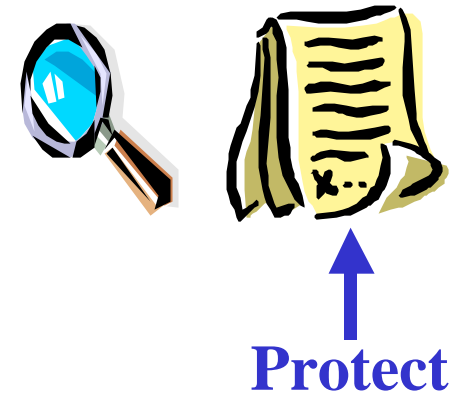


Digitally Signed Content

Parties have different goals



Protect



Protect

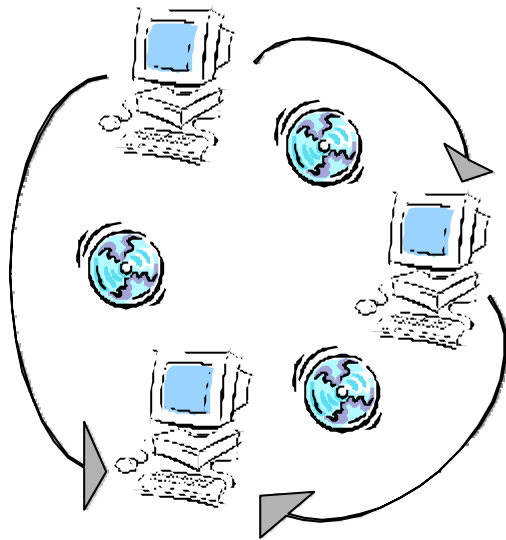
Fraud Considerations

Can't prove private key not compromised

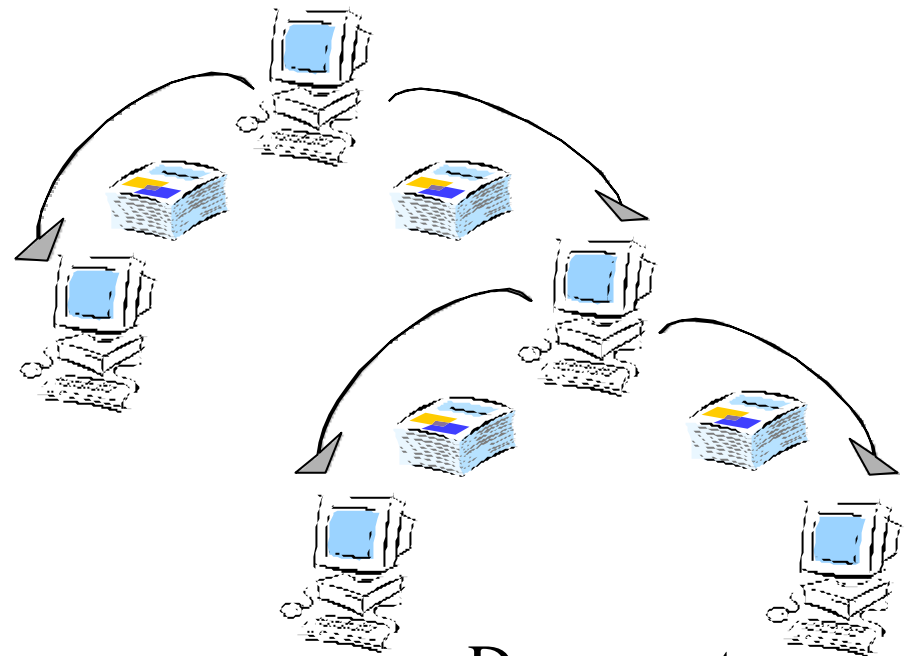
Long term protection of content

Trusted Content Distribution

Parties have common goals



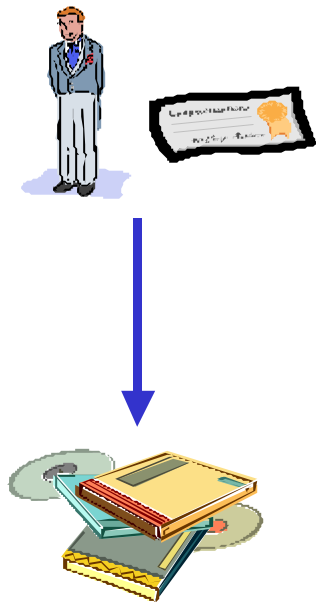
Applications
Updates
Security Patches



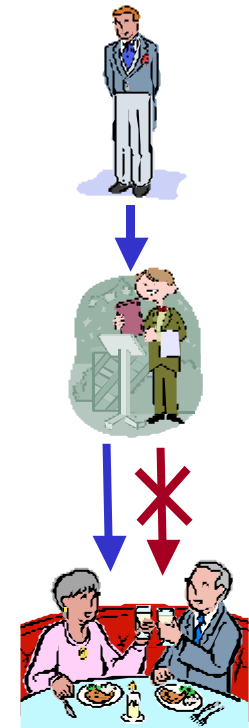
Documents
Reports

Controlling Access

Authorization Certificate
Gift Certificate
Capability (CAP ~1975)



Access Control List (ACL)
Dinner Reservation



Issues

Revocability
Accessibility Info
Complexity



Specific Thoughts

- Trustworthy digital certificate identities
- Protection for stored information
- Secure distribution of software & information



General Thoughts

- Examine business problems without specific PKI solutions in mind
- Consider complete system/environment
- Look at embedded PKIs
- Watch Jockey Club's eWin



Questions and Answers

Truth in Advertising

What PKI Can Really Deliver to Business

Thomas Parenty

President, Parenty Consulting, LLC

Author, *Digital Defense: What You Should Know About Protecting Your Company's Assets*

Hong Kong PKI Forum

15 September 2003