

A decorative graphic consisting of a horizontal row of eight colored squares (red, orange, yellow, green, cyan, blue, purple, magenta) and a vertical column of the same eight squares, forming an L-shape on the left side of the slide.

Economic Modeling and Risk Management in Public Key Infrastructures

David G. Masse / Chait Amyot
Andrew D. Fernandes / CryptoNym

A decorative graphic consisting of a vertical column of eight colored squares (magenta, purple, blue, cyan, green, yellow, orange, red) and a horizontal row of the same eight squares, forming an L-shape on the right side of the slide.

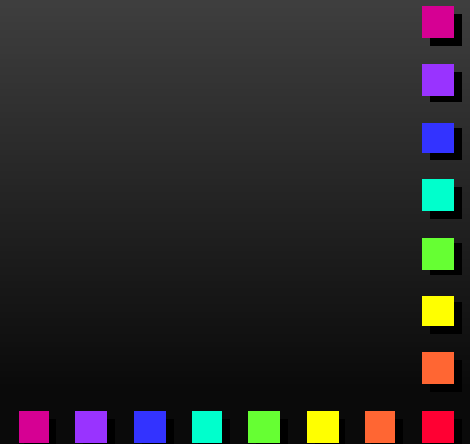
Open Networking

■ Defined as

- the Internet
- intranets
- Virtual Private Networks (VPNs)

■ Why the rush?

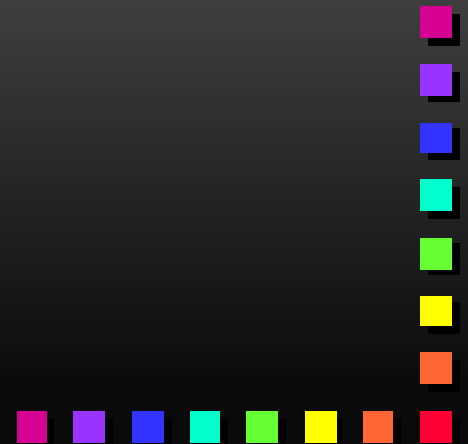
- cheaper
- faster
- more efficient



Open Networking Promises

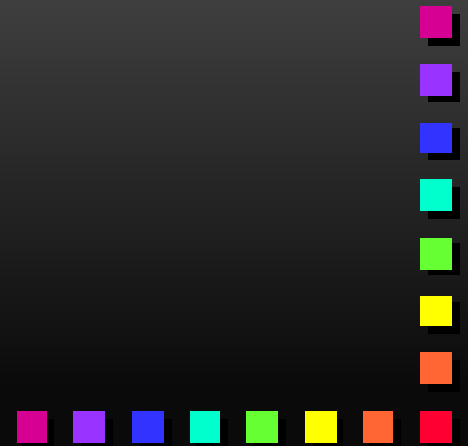
- Efficient, scalable information transmission
 - rapid electronic commerce
 - online payments and ordering
- But compare with
 - postal/courier services
 - fax machines
 - conference calls

It is a communication backbone!



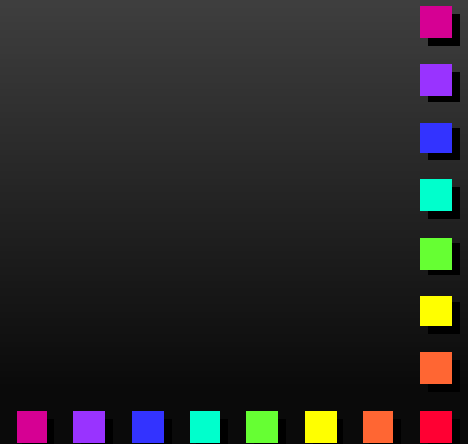
Analogue Voice: A Comparison

- Well understood and time tested
 - both theoretically and practically
 - Historically, its propriety and security were questioned
- Point-to-point fax communication
 - little legal or social controversy
 - usually considered “secure”



Line vs. Packet Switching

- Traditional telecom network
 - not extraordinarily secure
 - risk is understood for the bulk of transactions
- Open, packet switched network
 - much more efficient
 - efficiency achieved by its openness
 - this leads to a higher perceived risk



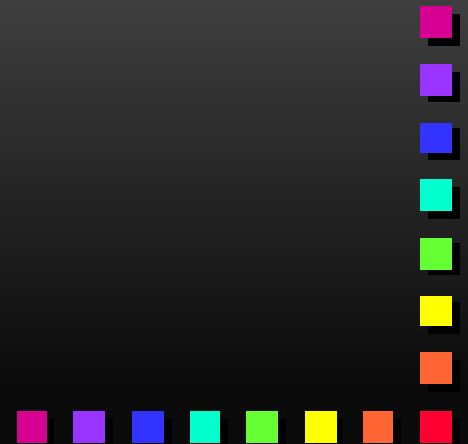
“Risk” and “Security”

■ Relative security

- confidentiality, integrity, authentication
- risk is always relative to the
 - value per transaction
 - maturity of the technology

■ Perception of risk

- objective is important
- subjective is equally so



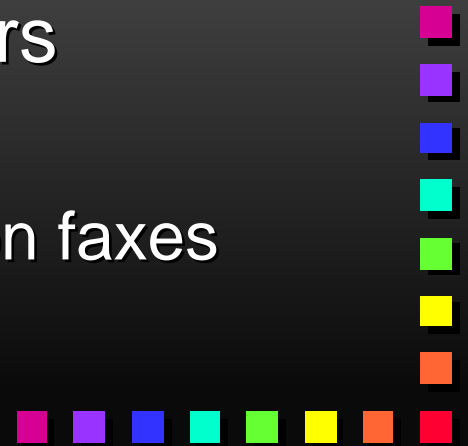
Again, the Telco Model

- Businesses have little concern with point-to-point voice & data communications
 - confidentiality
 - adequately addressed
 - integrity
 - comes from logical coherence of the message
 - authentication
 - comes from shared knowledge between parties



But Data? Really?

- Late 1970's - data transmission over voice lines becomes more widespread
 - data communications treated as voice
 - little perceived risk difference
- My bits and bytes look just like yours
 - faxes go to wrong numbers
 - digitized letterheads and signatures on faxes



Packet Switching

- No lingering familiarity with this medium
 - data can be transparently
 - diverted
 - copied
 - altered
 - replayed
 - can also happen to data on a line switched net
- So, is it really that insecure?
 - must handle the perceived risk



Scope of the Solution

- Linked to the scope of communication
 - digital commerce is important
 - as or possibly much more important
 - service industries (legal, financial, health care...)
 - non-commercial communications
- Confidentiality and integrity are not enough
 - authentication takes a central role
 - digital signatures are the answer



Public Key Infrastructures (PKIs)

- Legal and economic principles
 - must be discussed in the previous context
 - shift from paper/face-to-face to digital paradigm
- Must be
 - ubiquitous, easy to use and to **understand**
 - compliant to the needs of the key users
 - in all sectors of society
 - over the whole spectrum of types of communication



Public Key Management Services

- Diversity of needs dictates
 - a diversity of service providers
 - more than just a few “hierarchies”
- A PKMS must
 - clearly identify its own risks, and balance
 - expectation of profit
 - risk associated with earning that profit
 - clearly identify its client’s risks



Risk Management Techniques

- Avoidance
- Shielding
 - limitation of liability
 - contractual
 - legislative
- Acceptance and management
 - insurance, hedging, financing
- Success depends on effective and efficient risk management



PK Management Protocols

- Ubiquitous protocols are essential for
 - widespread use
 - efficient use
 - understanding its inherent risks
- Therefore, the **protocols** must be
 - easy to use and **understand**
 - compliant to the needs of the **all** key users



Existing PKI Paradigms

■ Current models

■ X.509v3

- distinguished names and other names

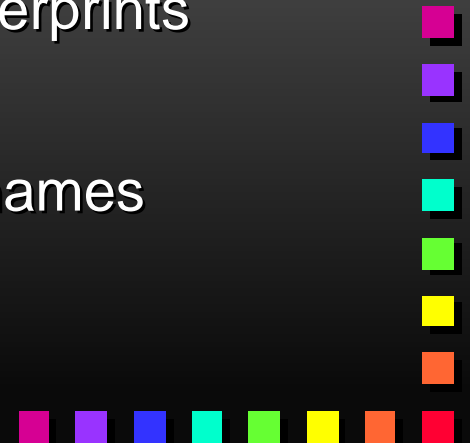
■ PGP

- email addresses, human names, PK fingerprints

■ SDSI

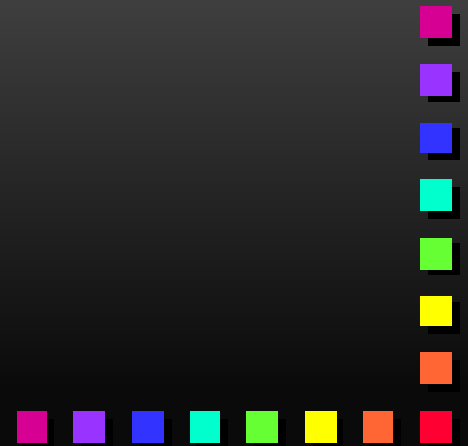
- principles are public keys with “human” names

What are the common elements?



Definition of a Digital Entity

- Minimal requirement
 - a unique secret key
 - needs no introduction
 - but who or what is “Entity 001010110101101”?
- Minimal **useful** requirement
 - secret key + an entity description
 - but descriptions need a context
 - context is given by the PKMS



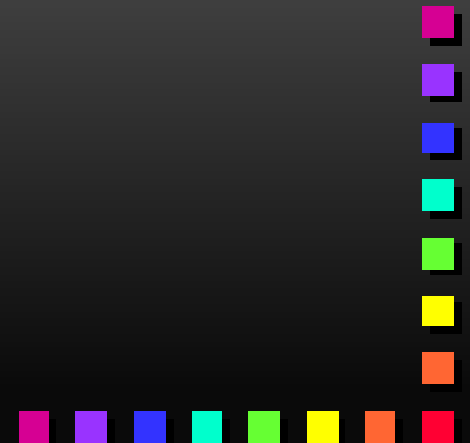
Entity Descriptions

■ Main purposes

- mnemonics, for us silly humans
- indexing, so the entity can be found
- accreditation, or “what the entity is allowed to do”

■ Identity vs. accreditation

- what identifies **you**?
 - your name, or
 - who you work for
- depends on who wants to know



Static and Dynamic Descriptors

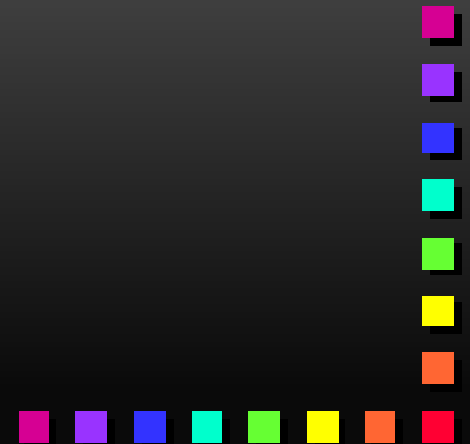
- Certain descriptors rarely change

- name
- birth date
- sex

- Some change relatively frequently

- postal address
- employer
- other accreditations

- The division is not always clear



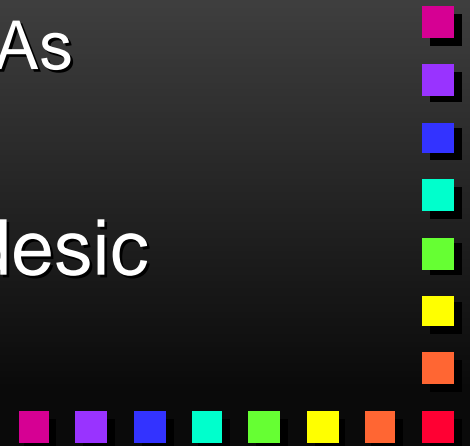
Architectural Elements of a PKI

- Current PKI protocols
 - concentrate on technical implementation
 - have little emphasis on
 - risk management
 - economics
- They should instead
 - shift the current “paper-paradigm”, not replace it
 - not be overawed by “unforgeable” digital signatures



Geodesics and Pyramids

- Current PK protocols
 - do not offer appropriate risk management
 - are therefore not economically efficient
- Major problem: pyramidal architecture
 - complex interdependency between CAs
 - risk is concentrated toward the apex
- Real open networks are more geodesic
 - example: a telephone book



Flattening the Hierarchies

- Current PKIs tend toward pyramids
 - they are neat, tidy, and highly functional
 - most efficient with centralized control
- Difficulties come when pyramids must be interconnected
 - too much consensus is required
 - the hierarchy begins to impose its requirements on the organizations, instead of *vice versa*



Real Life Examples

Low-tech

- Telephone books
- Identification is by
 - telephone number
 - names
 - addresses
 - logos
- One book covers
 - large array of services
 - large geographic area

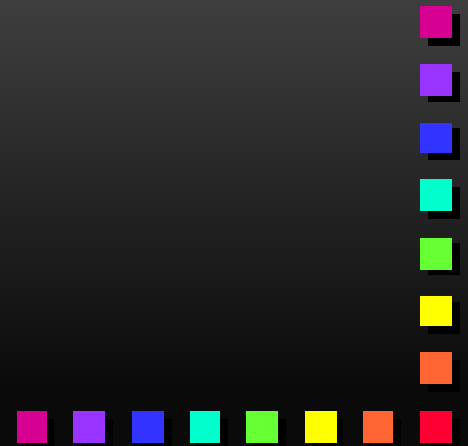
High-tech

- The Internet
 - TCP/IP is logically pyramidal
 - DNS flattens this out
- Identification is by
 - domain names
 - host names
 - usernames



PKIs Must be Nonpyramidal

- Can the world be organized pyramidally under just one or a few “trusted” entities?
- Is it acceptable that key-compromise in one organization can have drastic and far reaching effects?



Reasons for Decentralization

- The CA cannot do it all
 - identify
 - accredit
 - generate/assign/manage keys
- Clients feel strongly about
 - providing and accepting their own accreditations
 - managing the risk themselves
 - having the level of security match their organizational resources



Consequences of Decentralization

- Risk is distributed
 - root key compromise is no longer catastrophic
 - less reliance on “inter-CA guidelines”
- The ability to manage the risk is placed where the risk lies (avoidance)
- The services will then fit the needs, instead of having the needs fit the services



Economic Consequences

■ For the PKMS

- less to do = cheaper, easier to provide service
- easier to implement security
- manageable risk in providing the service

■ For the Client

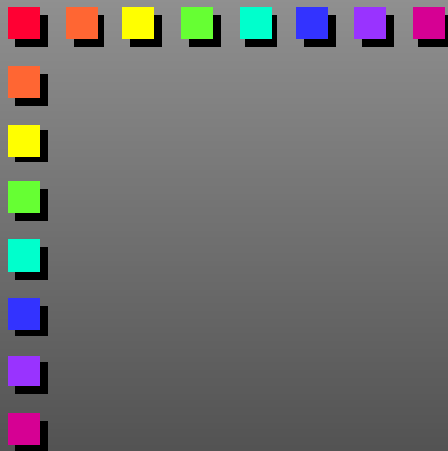
- more comfortable paradigms = faster acceptance
- lower cost of risk management
- manageable risk in utilizing the service



Conclusions

- Efforts to develop a PKI should concentrate
 - on shifting current paradigms, not replacing them
 - on providing appropriate vehicles for risk management
- Organizational structures should
 - more closely match how real interorganizational communication occurs
 - accommodate a broad range of client needs





David G. Masse

DMasse@Chait-Amyot.CA
+1 514 879 1353 extension 217

Andrew D. Fernandes

Andrew@CryptoNym.Com
+1 519 433 5026

<http://www.chait-amyot.ca/docs/pki.htm>

