D. Nagy and N. Shakel:

OpenPGP-based Financial Instruments and Dispute Arbitration

Financial Cryptography and Data Security 2008

January 31,Cozumel, Mexico

Motivation

- **Impediments to Electronic Commerce**
  - Legal costs typically exceed transaction value
  - No shared jurisdiction, often poor local laws
  - Expensive reputation signals
- **Traditional Solution to Analogous Problems**
  - Lex Mercatoria

Utilizing OpenPGP

- **Purpose**
  - – Digital financial instruments and supplements
  - – Credit reputation tracking
- **Available infrastructure**
  - – Standard specification (RFC4880)
  - – Public Key Server (PKS) network

Design Goals

- **Closely match traditional solutions**
  - Highly evolved stuff, centuries of experience
  - Useful metaphors, ease of acceptance
- **No exotic cryptography**
  - Common crypto concepts are difficult enough
  - No standard implementations

Important distinctions

- **Irreversible operations**
  - Traditionally: marking paper with ink
  - Digitally: publishing a secret
- **Confidentiality protection**
  - Traditionally: reactive
  - Digitally: proactive

Irreversible marking

- **Procedure**
  - – Include the hash value of a random secret in the signed document (along with semantics)
  - – Publish the pre-image
- **Main advantage**
  - – Unconditional confidentiality

Example: Money Order

- **Most important fields**
  - Amount, currency
  - A hash value (the pre-image goes to recipient)
  - Digital signature with timestamp
- **Execution**
  - Exchange cash for pre-image

Potential

- **A complete digital marketplace like eBay**
- **Features**
  - Listings, auctions, *feedback*
  - Shipping, payment security
  - Dispute resolution (speedy, cheap justice)
  - Decentralized, reliable infrastructure

Dispute Resolution

- **Prevent disputes, whenever possible**
- **Reputation: signatures on PGP keys**
- **Sufficient evidence**
- **If necessary: Arbitration**
  - – Arbitration clauses in contracts
  - – Arbitration services

Arbitration Setting

- **Dramatis Personæ**
  - Alice (claimant) & Bob (respondent)
  - Justin (arbiter)
- **Capabilities**
  - Alice and Bob have public keys and computers
  - Justin has a 24/7 server infrastructure

Arbitration Procedure

- Alice feels cheated, submits claim w/ evidence (typically chosen from a menu), pays Justin
- Justin (automagically) notifies Bob
- Bob is faced with a choice:
  - Settle, Contest, Demur or Do Nothing

Problems

- **Sybil attacks**
  - – Negative reputation can be thrown away
  - – Spoils of fraud can be transferred to untainted identities
- **Non-digital evidence**
  - – Turning it into digital evidence is expensive

Thank You!