Utilizing and Enhancing the strengths of IBE
Security in the real world

Agenda

- Timeline
- Focusing IBE on what it is good for
- Demands of the big wide world
Timeline

1984  Adi Shamir proposes IBE concept
1998  Cliff Cox Quadratic Residues
1999  Sakkai & Kasahara solve the maths
2000  Boneh & Franklin add security proof
2001  Student projects at Bristol University
2003  Spin out company launched ("Argelcom")
2005  Argelcom renamed "Identum"
2008  Identum acquired by Trend Micro
2009  Trend Micro release fully integrated IBE portfolio

FOCUSING ON WHAT IBE IS GOOD FOR...
Don’t copy PKI

Wrong with PKI
- The infrastructure is costly to install and maintain
- Creates cryptographic islands
  - The modern world doesn’t work that way
- Expects users to understand security
  - They don’t
  - They don’t want to!

Right with IBE
- Vastly reduced key handling
  - Easy to scale a single key server to work for everyone
  - 2 keys to talk to the world
- A great invention because it doesn’t change the way you work!

IBE strength is key handling, not encryption

- “if it ‘aint broke don’t fix it”
  - Symmetric encryption for the data
  - IBE for the encryption keys

(i.e. do KEM/DEM)
Simplicity in implementation

- Model user experience on their existing process
- So for email:
  - Read / Compose in the normal email client
  - Push out the content – don’t pull back to a server to read
  - Online or offline

- Universal reach
  - Desktop
  - Gateway
  - Hosted
  - Mobile
  - Browser

Integration with other elements

- Email hygiene
  - AV
  - Spam
  - Sender reputation

- Data Leak Protection

- Access control

- Workflow
  etc