Proxy Re-encryption

Phill Hallam-Baker

What it is

- Alice sends a encrypted message to X (e.g. a cloud service)
  - Public key ‘belongs to’ X
  - X cannot decrypt the message
  - But X can convert messages
    - Forward message to B, C, D using re-encryption keys
  - Holder of private key creates re-encryption keys
    - This can be performed offline

- Can be implemented in any DH cryptosystem
  - Including EC variants

Why is it useful

- Confidential mailing list
  - Cloud service and only cloud service knows membership
  - Cloud service can’t decrypt message, not a point of vulnerability
- IMAP / POP server
  - Alice has 5 devices, wants end to end encryption to each one
  - Senders do not want to have to provide 5 decryption blobs
- Implement label based security CRM scheme
  - Very powerful, currently encumbered, patents ‘should’ expire soon
- Group chats…

Next Steps

- Well known in theory circles
  - Well grounded
  - Has been overlooked by protocol community
    - No standards support
    - No (direct) support in toolkits

- Open questions
  - What are the best approaches that are not encumbered?
  - How should this be expressed in key formats?