Voltage security

XL Global Services: A Data Privacy Case Study

Presented by:
Mark Schertler
December 2006

XL Capital Ltd

- Corporate Information
  - Global Insurance, Reinsurance, Financial Risk Specialists
  - 3500+ Users in 78 Offices in 29 Countries
  - Consolidated Assets of ~$59.8B
    - as of Sept. 30, 2006
  - Member S&P 500
- Tom Dunbar
  - Global IT Chief Security Officer
  - 2006 SC Magazine CSO of the year

Key Concerns

- Privacy regulations compliance across 29 countries
- 3 different e-mail systems (growth thru acquisition)
- End user ease of use
  - Internal (office-to-office) encryption
  - External (outside firewall) encryption
    - B2B
    - Customer
- Mobile BlackBerry devices
- Administrative Overhead
- Disaster Recovery
- 3,500+ user deployment

Additional Drivers

- Protection on the server
  - E-mail protected on mail server as well as in motion
- Searchability
  - Message recovery for legal / regulatory compliance
- Encryption schema strength
  - 80, 112, 128 bit equivalents
- Attachments
  - Automatically encrypt all attachments
- Visibility
  - Info on who receives message

Evaluated Solutions

- Traditional PKI
  - Implementation and manage overhead greater than our globally decentralized corporation could handle
    - IT staff in every office (78) to effectively manage
  - Certificates, CRL unwieldy
- Voltage SecureMail
  - Simple end-user experience – “Send Secure” button
  - Decryption and signature verification at the laptop
  - No additional staff
  - Low infrastructure overhead
  - Scalable as companies grows through acquisition
  - Policy-based Encryption
  - Low cost-of-ownership

Identity-Based Encryption

Basic Idea: Public-key Encryption where Identities are Public Keys

- **IBE Public Key:**

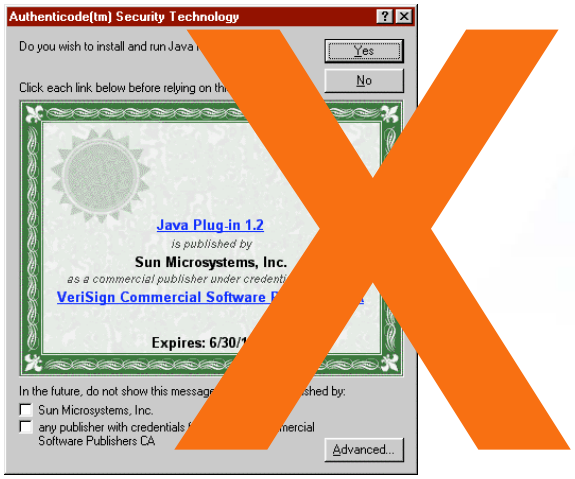
  alice@gmail.com

- **RSA Public Key:**

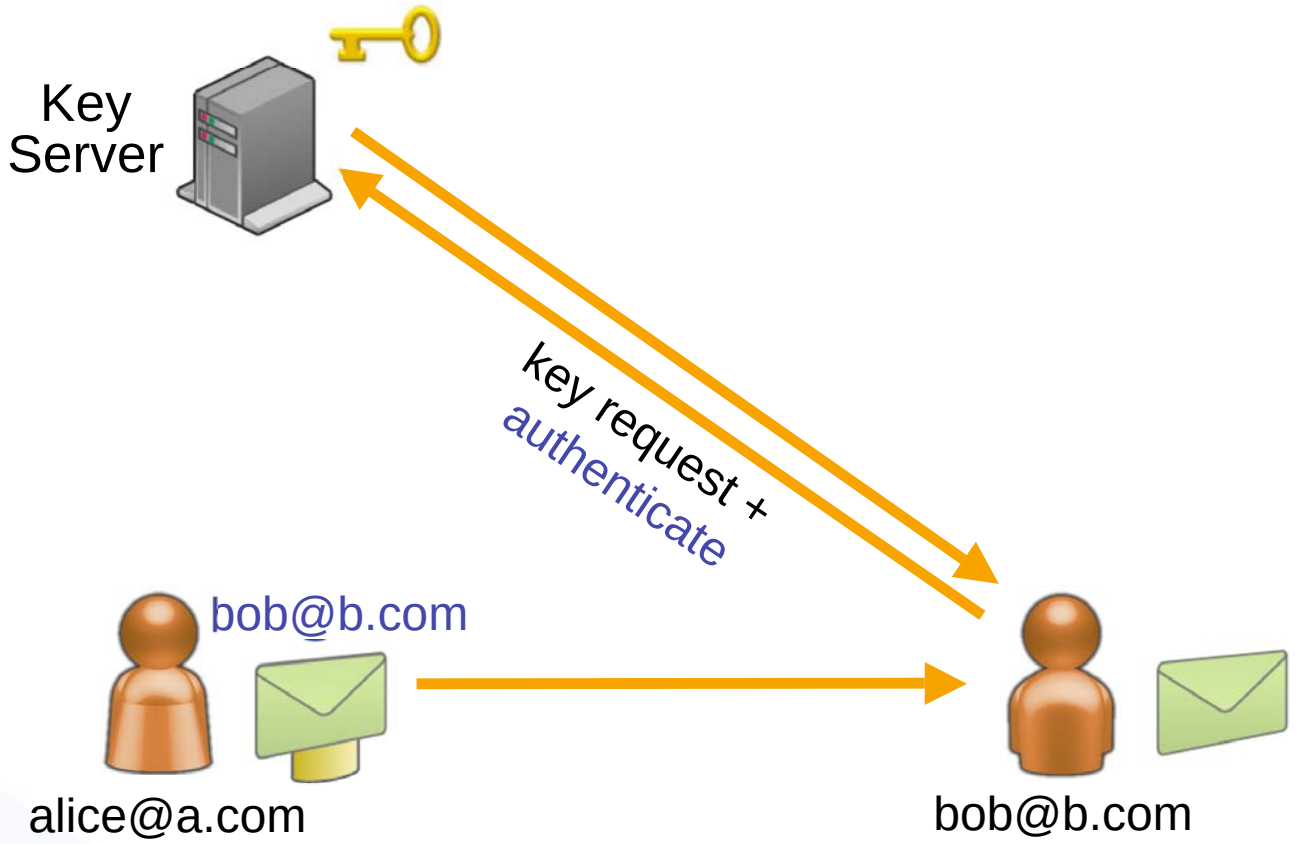
  Public exponent=0x10001
  Modulus=135066410865995223349603216278805969938881475605667027524485143851526510604859533833940287150571909441798207282164471551373680419703964191743046496589274256239341020864383202110372958725762358509643110564073501508187510676594629205563685529475213500852879416377328533906109750544334999811150056977236890927563

IBE does not need certificates

- Certificates bind Public Keys to Identities
  - e.g. bob@b.com has key 0x87F6…
  - Signed by a Certification Authority
- In IBE, Identity and Public Key is the same
  - No certificate needed
  - No certificate revocation
  - No certificate servers
  - No pre-enrollment



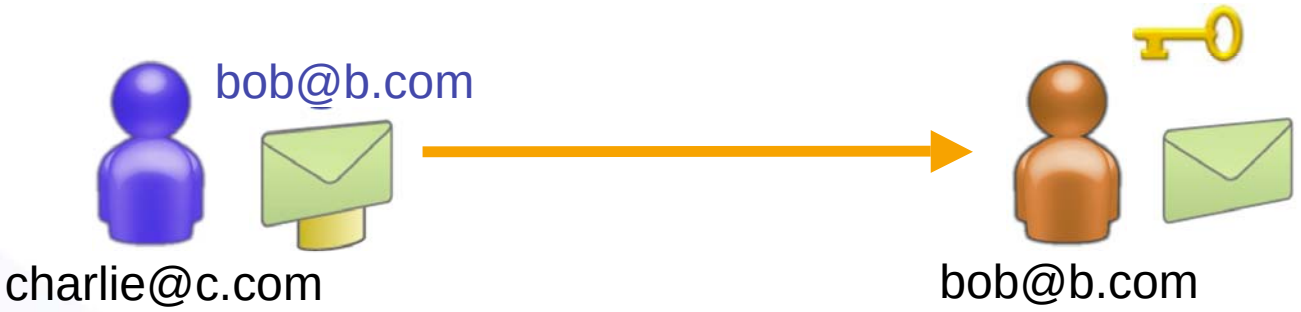
How IBE works in practice
Alice sends a Message to Bob



How IBE works in practice
Second Message to Bob

Key Server

Fully off-line - no connection to server required



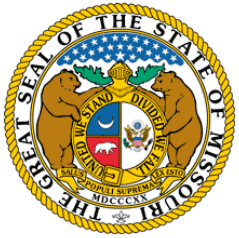
XL Capital Deployment

- Voltage Key Management Server
  - 2 Redundant 1U servers
  - Deployed at Central IT Location
    - Easy access and management
- Voltage SecureMail Blackberry
  - Plugin for Blackberry Enterprise Server
- Voltage SecureMail Clients
  - All 3500 employees deployed in weeks
  - 1/3 laptops users
    - Providing e-mail at rest security

Summary

- XL Global Services policy requires confidential information be protected at all times including when sent via email.
- As a global organization a flexible solution that can comply with the various laws and regulations enacted throughout the world that impact both the security and privacy of information was required
- Reviewed a number of different options including traditional PKI
- Concluded “Voltage Key Management Server would provides a usable, scalable, low cost-of-ownership solution that supports our policy, regulatory, and budgetary requirements.”

A Few Additional Voltage Enterprise Customers



More Information

- Computer World – June 12, 2006 article
  - Seven keys for complete message security
- SC Magazine – March 6, 2006 article
  - CSO of the year: Thomas Dunbar, global chief security officer, XL Capital

Questions?