

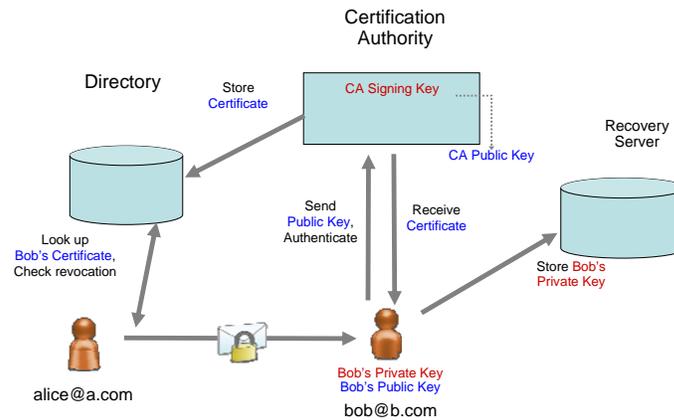
The Case for IBE

Terence Spies
CTO, Voltage Security

The State of Encryption

- Certificate based encryption is problematic
 - Basic issue: need a certificate to encrypt
 - *User impact*: need to preregister, need to locate certs
 - *Network impact*: need to expose a directory
 - *Policy impact*: data recovery requires an extra layer
- Numerous attempts to re-engineer
 - SPKI, "Plug and Play PKI", "user-centric PKI"
 - Make signature and auth better, no fix for public key location problem

PKI Architecture



IBE

•“An identity-based scheme resembles an ideal mail system: If you know somebody’s name and address you can send him messages that only he can read.... It makes the cryptographic aspects of the communication almost transparent to the user, and it can be used effectively even by laymen who know nothing about keys or protocols.”

•Adi Shamir, *Identity-based Cryptosystems and Signature Schemes*

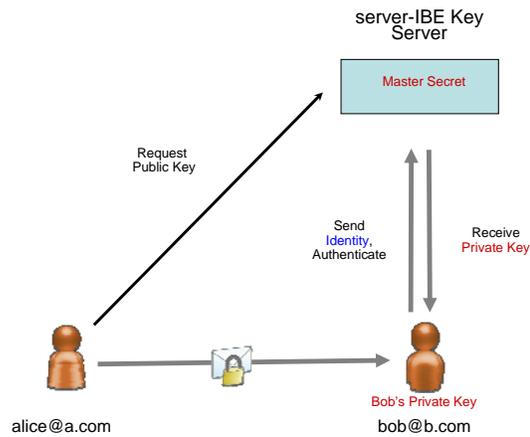
•Conventional crypto “emulation”

- Microsoft Active Directory, “Enroll on Behalf”
- Boneh and Tsudik, “Mediated RSA”
- Callas, “IBE with Conventional PKI”

•Pairings give a fully-functional IBE

- Boneh and Franklin, “IBE from the Weil Pairing”

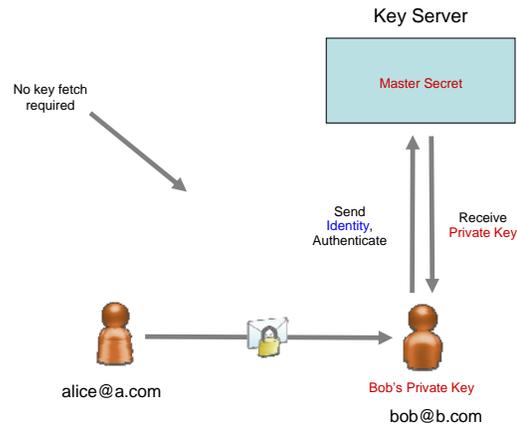
IBE “emulation”



IBE Emulation

- Solves some PKI encryption issues
 - Eliminates the need for pre-enrollment
 - Inherent key recovery
 - Can retains some compatibility with certs and directories
- Retains disadvantages of Kerberos
 - Requires online access to server to encrypt
 - Have to operate security critical pseudo-directory
 - Impractical at 256 bit security levels (15,360 key gen)

Pairing IBE



Pairing-based IBE

- Solves the public key fetch problem
 - Eliminates the need for pre-enrollment
 - Public server only needs to serve a single static data item
 - Allows for offline encryption to any key
 - Supports short-lived, revokable keys
 - Inherent key recovery
- Requires new cryptography

Summary

- **PKI solves many problems**
 - Machine encryption (SSL)
 - Digital signature, authentication
- **PKI has a fundamental flaw for user encryption**
 - Need a way to find a public key given an identity
 - Pairing based IBE is the most elegant way to fix this problem