Identity-Based Encryption

Guido Appenzeller (CTO)
Terence Spies (VPE)

Voltage security

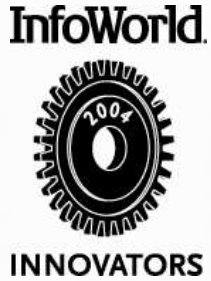
Identity-Based Encryption (IBE)

Ok, so we have (yet another) new encryption algorithm, why on earth should we care?

1. It's not about more security, it's about making encryption much easier.
2. Industry is adopting it, since it solves difficult, practical problems
3. It might help you solve a number of the problems associated with PKI (key lookup, certificate directories, revocation…)

Awards for Voltage IBE Solutions

- Bank Technology News “Top Ten Technology Companies” - August, 2003
- Network World “Tops in Innovation” - February, 2004
- InfoWorld Innovators Award - May 2004
- AlwaysOn “Top new innovator company” – July 2004



Voltage security

Identity-Based Encryption (IBE)

Basic Idea: PKI where Identities are Public Keys

- e.g. my public key is the string “guido@voltage.com”

Advantage: Vastly simplified Encryption Key Management

- No more certificates, certificate look-ups and certificate directories
- Dramatically simplifies key revocation issues
- (Less dramatic simplifications for signing/authentication)

If you have deployed PKI, IBE can help you:

- Easily extend PKI authentication to encryption
- It provides a lightweight keying infrastructure to communicate with people outside your PKI

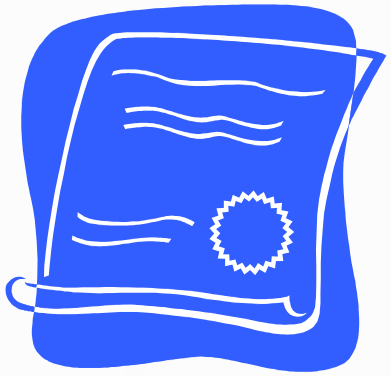
Agenda

1. Identity-Based Encryption
   - What it is, how it works
   - Advantages
2. How can IBE help you with your PKI
3. Question & Answer

Identity-Based Encryption (IBE)

Public-key Encryption where Identities are used as Public Keys

Example:



- IBE Public Key:

  alice@gmail.com

- RSA Public Key:

Public exponent=0x10001

Modulus=135066410865995223349603216278805969938881475605667027524485143851526510604859533833940287150571909441798207282164471551373680419703964191743046496589274256239341020864383202110372958725762358509643110564073501508187510676594629205563685529475213500852879416377328533906109750544334999811150056977236890927563

Identity-Based Encryption (IBE)

- IBE is an old idea
  - Originally proposed by Adi Shamir, co-inventor of the RSA Algorithm in 1984
  - Not possible to build an IBE system based on RSA
- Only recently the first practical implementation became available
  - Boneh-Franklin Algorithm published at Crypto 2000
  - Developed under a DARPA program
  - Based on well-tested building blocks for encryption (elliptic curves and pairings)
- Other algorithms exist
  - Quadratic-Residue (2001), Boneh-Boyen (2004)

A Selection of Papers on IBE

- Identifier Based PKC - Potential Applications
  - I. Levy. Invited talk at the 1st Annual PKI Research Workshop 2002, 2002.
- Two Remarks on Public Key Cryptology
  - R. Anderson. Invited talk at the ACM Conference on Computer and Communication Security, ACM-CCS 1997, 1997.
- Towards an Identity Based PKI
  - D. Boneh. Invited talk at the 1st Annual PKI Research Workshop 2002, 2002.
- An Identity-Based Key-Exchange Protocol
  - C. G. Gunther. In Proceedings of Eurocrypt 1989, Lecture Notes in Computer Science, Springer-Verlag, pp 29-37, 1989.
- Identity-Based Encryption: a Survey
  - M. Gagne. RSA Laboratories Cryptobytes, Vol 6, No 1, pp 10-19, 2003.
- Simple Identity-based Encryption with Mediated RSA
  - X. Ding and G. Tsudik. To appear in Proceedings of RSA Conference 2003, Cryptographer's Track, CT-RSA '03, 2003.
- Non-interactive Public-key Cryptosystem
  - U. Maurer and Y. Yacobi. In Proceedings of Eurocrypt 1991, Lecture Notes in Computer Science, Vol 547, Springer-Verlag, pp 498-507, 1991.
- Identity-Based Encryption from the Weil Pairing
  - D. Boneh and M. Franklin. In Proceedings of Crypto 2001, Lecture Notes in Computer Science, Vol 2139, Springer-Verlag, pp 213-229, 2001.
- An ID-based Cryptosystem based on the Discrete Logarithm Problem
  - S. Tsuji and T. Itoh. IEEE Journal on Selected Areas in Communication, Vol 7, No 4, pp 467-473, 1989.
- Cryptosystems Based on Pairings
  - R. Sakai, K. Ohgishi and M. Kasahara. In Proceedings of Symposium on Cryptography and Information Security, SCIS 2001, 2001.
- Identity Based Encryption from the Tate Pairing to Secure Email Communications
  - M. Baldwin. Master of Engineering Thesis, University of Bristol, 2002.
- Towards Practical Non-interactive Public Key Cryptosystems using Non-maximal Imaginary Quadratic Orders
  - D. Huhnlein, M. Jacobson and D. Weber. In Proceedings of 7th Workshop on Selected Areas in Cryptography, SAC 2000, Lecture Notes in Computer Science, Vol 2021, Springer-Verlag, pp 275-287, 2000.
- A Realization Scheme for the Identity-based Cryptosystem
  - H. Tanaka. In Proceedings of Crypto 1987, Lecture Notes in Computer Science, Vol 293, Springer-Verlag, pp 341-349, 1987.
- Towards Hierarchical Identity-Based Encryption
  - J. Horwitz and B. Lynn. In Proceedings of Eurocrypt 2002, Lecture Notes in Computer Science, Vol 2332, Springer-Verlag, pp 466-481, 2002.
- The Weil and Tate Pairings as Building Blocks for Public Key Cryptosystems
  - A. Joux. In Proceedings of ANTS, Lecture Notes in Computer Science, Vol 2369, Springer-Verlag, pp 20-32, 2002.

IBE does not need Certificates

- Certificates bind Public Keys to Identities
  - e.g. bob@b.com has key 0x87F6…
  - Signed by a Certification Authority

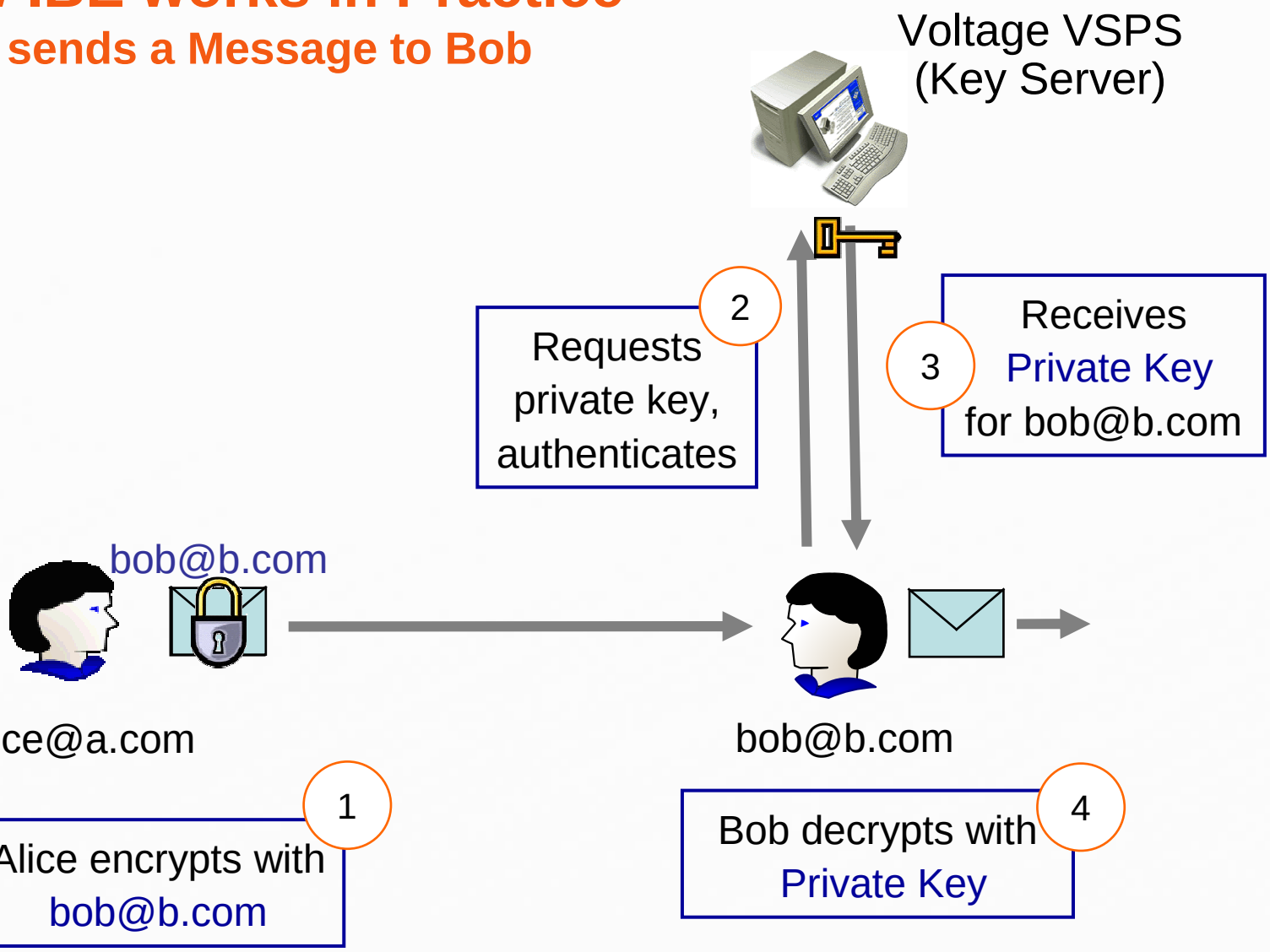
- In IBE, Identity and Public Key is the same
  - No certificate needed
  - No certificate revocation
  - No certificate servers
  - No pre-enrollment

- IBE can also handle attributes
  - I will later show you how

Voltage security

How IBE works in Practice

Alice sends a Message to Bob



Voltage security

How IBE works in Practice

Charlie sends a Message to Bob

Voltage VSPS
(Key Server)

Fully off-line - no connection to server required

charlie@c.com

bob@b.com

1

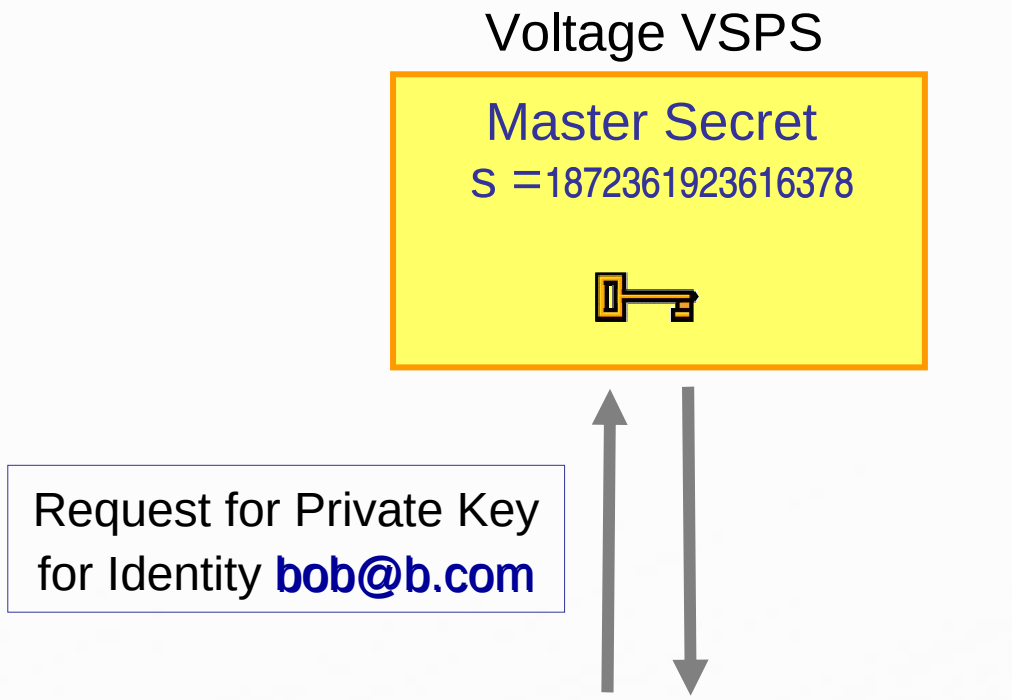
Charlie encrypts with bob@b.com

2

Bob decrypts with Private Key

Voltage security

The IBE Key Server
(Voltage VSPS)



- Key Server has “Master Secret” to generate keys
  - A random secret is picked when the server is set up
  - Each organization has a different Master Secret
  - Private key is generated from Master Secret and Identity

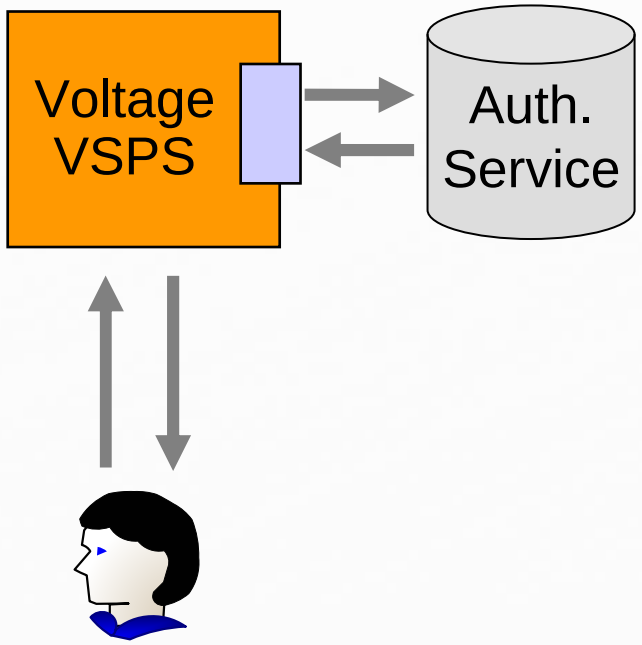
User Authentication for IBE

Authentication needs differs by Application and User

- More sensitive data, requires stronger authentication
- Different classes of users may authenticate differently
- Identity-Based Encryption scales across all levels

Authentication Adapters

- PKI Smart Cards
- RSA SecureID
- Client Certificates
- LDAP, Active Directory
- Login/Password
- Email Answerback



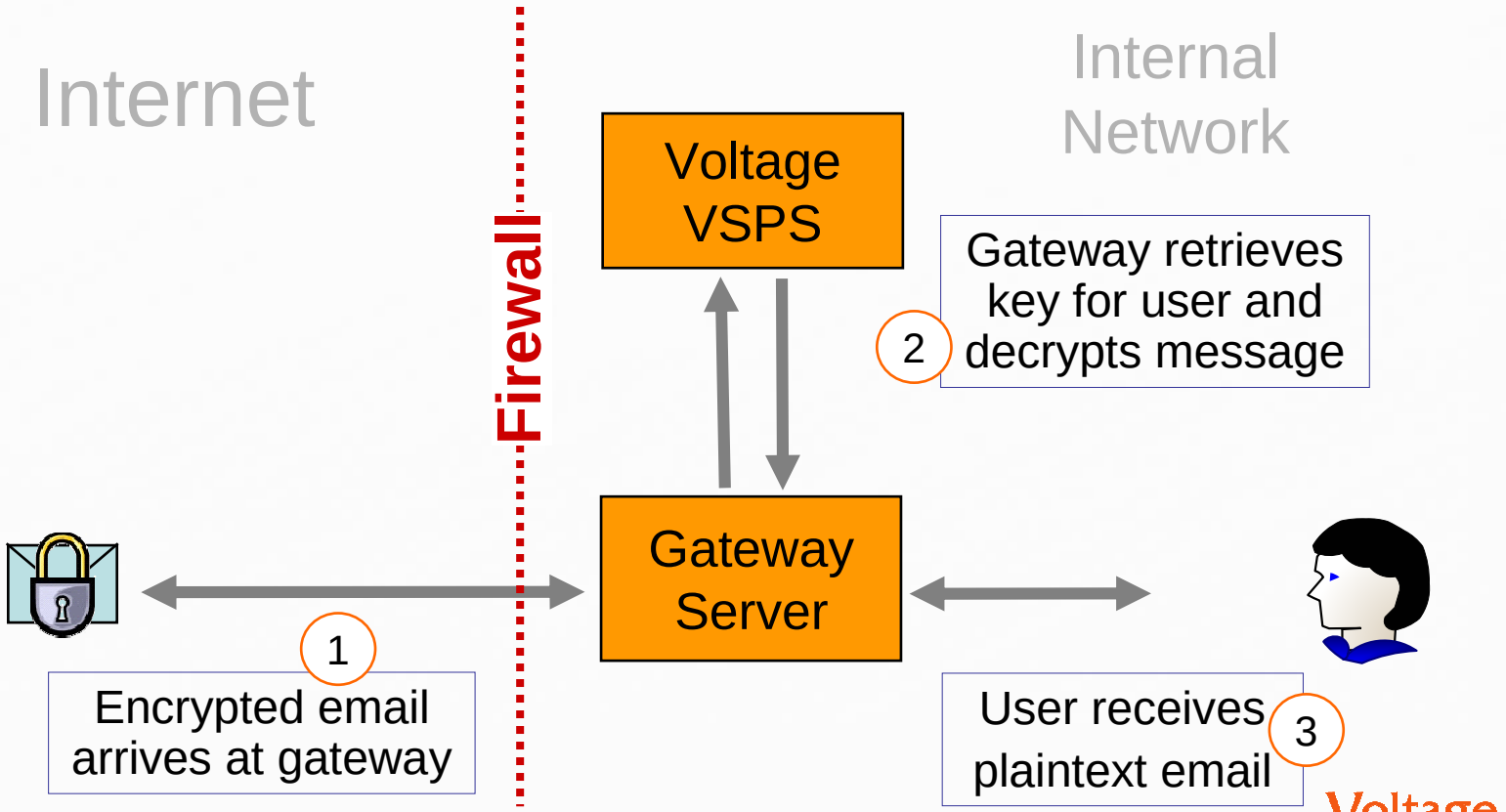
Key Revocation, Expiration and Policy

- Key validity enables revocation – “key freshness”
  - Every week public key changes, so every week a new private key is issued → revocation can be done on weekly basis
  - Refresh period is configurable
- Key can contain other policy: user attributes, group names, policy information for more sophisticated authentication options

IBE is well suited for Perimeter Encryption

The Voltage Gateway Server

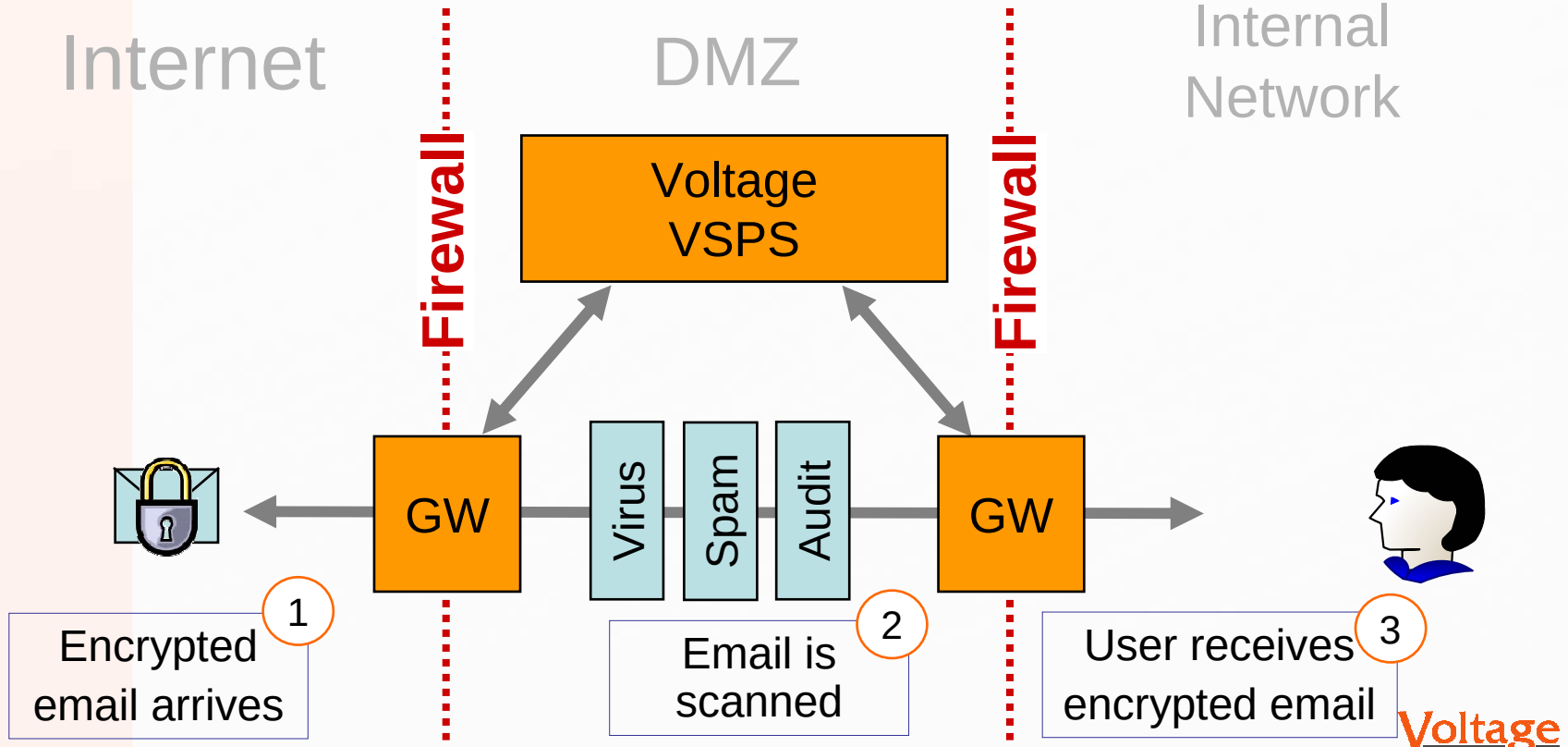
- Encrypt/Decrypt Mail at the Firewall
  - Gateway requests keys from Key Server (VSPS)
  - No client deployment required inside the organization
  - Encryption can be done via policy



IBE allows Perimeter Content Scanning

Filtering Spam and Viruses with End-to-End Encryption

- IBE's on-the-fly key genaration capability enables end-to-end encryption with content scanning
  - Filter for Virusses, Trojans, Spam etc.
  - Allows archieving email for compliance, audit



Advantages Of IBE, Part I

- No certificates
  - No certificate lookup
  - No costly infrastructure: no cert directories, CRLs, etc.
  - No information leakage
  - No parallel identity store: leverages existing identity information
- True public-key crypto system
  - No per-message keys
  - No mirrored message stores
  - Architected for “occasionally-connected” user

Advantages Of IBE, Part II

- Simplified revocation
  - Keys expire on weekly basis
  - No additional work to remove user access
- On-the-fly key generation
  - Key roaming
  - Archiving/scanning/data recovery
- Dynamic group management and access control
- Scalability
  - No per-message or per-user state
  - On-the-fly key generation means no key archival required
  - Backup for Disaster Recovery is can be done on a single floppy

Agenda

1. Identity-Based Encryption
2. How can IBE help you with your PKI
    1. Lightweight External Security
    2. Scalable Encryption for PKI
3. Question & Answer

Public Key Infrastructure

- PKI for authentication is being widely adopted in the Federal Government
  - Smartcards based solutions, e.g. CAC, TWIC
  - HSPD-12/FIPS 201 will accelerate this further

- However, problems remain
  - Deployment is expensive and non-trivial
  - Certificate Revocation (CRLs, OCSP)
  - Certificate Servers leak Information
  - Little adoption for Data Encryption
  - Key Recovery (e.g. for filtering mail for viruses) remains a Problem
  - Unclear how to extend it beyond the borders of the organization

IBE and PKI - Complementary Strengths

PKI with Smart Cards

- Maximum security through hardware tokens
- Works well for signing/authentication
- Requires roll-out
  - generate keys for users
  - distribution of smart-cards

Sweet Spots for PKI

- Authentication
- Signing
- Inside the organization

Identity-Based Encryption

- Good for encryption
  - no key-lookup
  - revocation is easy
- Ad-hoc capable
  - requires no pre-enrollment
  - software only
- Content scanning easy

Sweet Spots for IBE

- Encryption
- Inside and outside the organization

Two Models for Deploying IBE

1. **External** - To communicate securely with people that are not enrolled in your PKI
   - Use PKI internally
   - Use IBE and short-lived signing certificates to secure external communications
   - Extremely lightweight and easy to use, users can be enrolled in minutes

2. **Hybrid** - To add scalable, easy-to-manage encryption to your existing PKI deployment
   - PKI for authentication/signing, IBE for encryption
   - No key-lookup, no leaking of data, simplified revocation

Not everyone is enrolled in a PKI

External

- Inside the Federal Government, PKI is becoming ubiquitous

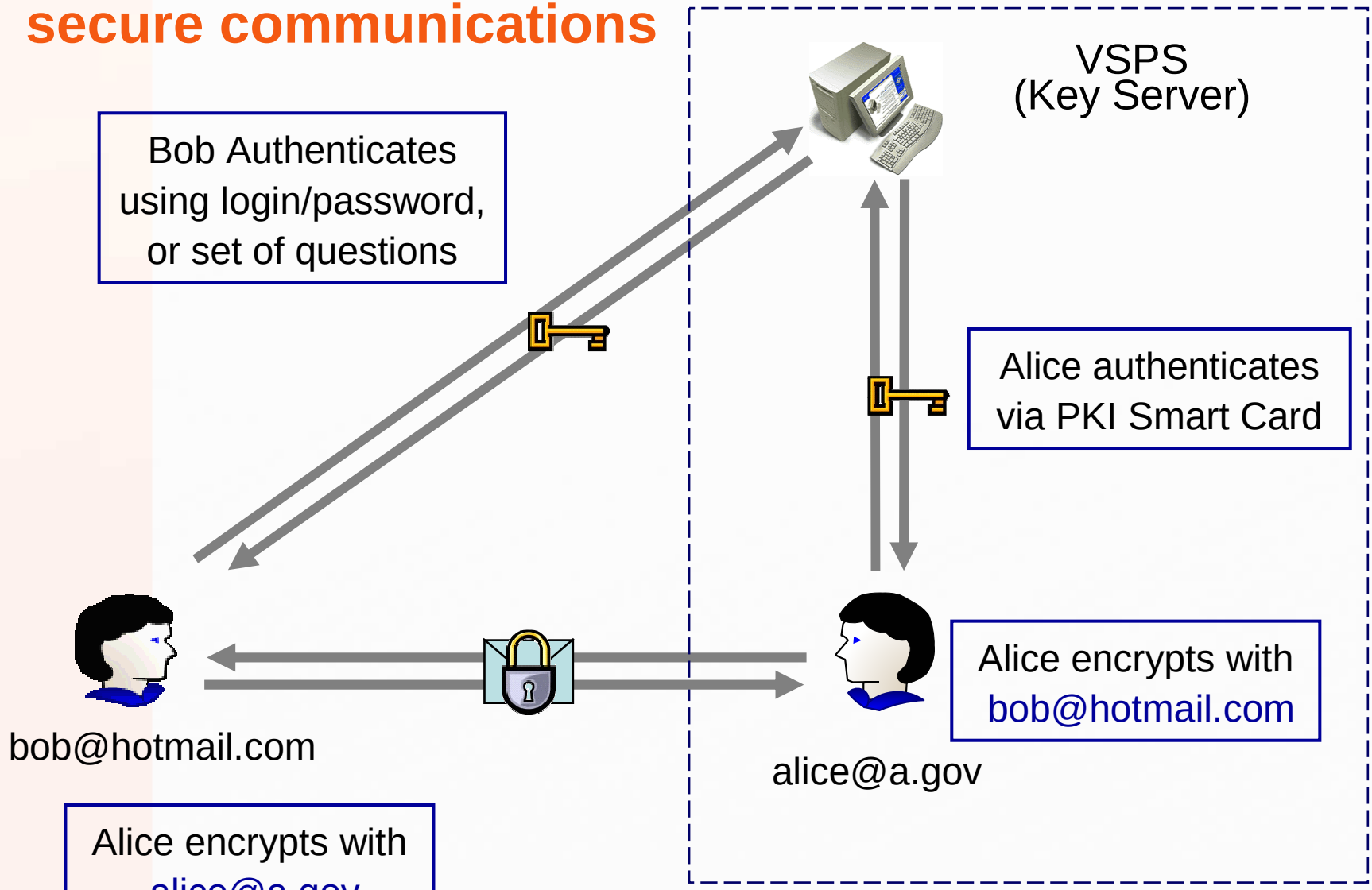
- However, organizations communicate with many parties that do not have PKI deployed

  Examples:

  - Suppliers, Service Providers
  - Local Police, Fire Departments
  - Dependents of Federal Employees
  - Retired Employees
  - Dynamic Coalitions, International Allies
  - …

PKI with IBE for external secure communications

External



Voltage security

PKI with IBE for external secure communications

External

- Inside your Organization, use PKI
- With external People, use IBE

Advantages:

- Ad-Hoc Capable, external users don't need to be enrolled before you can communicate with them
- Different Authentication mechanisms for different users (PKI, passwords, delegated etc.)
- Build in key revocation (e.g. no CRLs required)
- Content scanning for Viruses, SPAM, Spyware works out of the box
- No certificate servers required
- Much lower complexity
- Much lower total cost of ownership

Hybrid Model - Combining IBE and PKI

- PKI users use IBE private key for decryption
  - PKI Private key is used for Signing and Authentication (including IBE key request)
  - Email address is used for Encryption
  - IBE Private key is used for Decryption

- Advantages:
  - System is fully off-line capable (no key lookup)
  - No certificate servers required
    - No leaking of information
  - No escrow servers required
  - Content scanning is simplified

Hybrid IBE/PKI Workflow

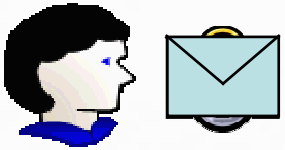
VSPS
(Key Server)

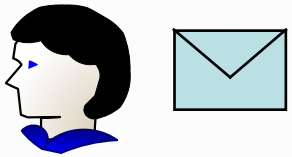
Bob authenticates with PKI Key

2

3

Bob receives IBE Private Key for bob@b.com





alice@a.com

1

Alice sends email to Bob:

IBE-Encrypt with: bob@b.com
PKI-Sign with: PKI Key

bob@b.com

4

Bob decrypts email with IBE Private Key
verifies signature with PKI

Summary

Identity-Based Encryption

- All the advantages of PKI without certificates
- Ad-Hoc capable, no pre-enrollment required
- Very user friendly
- Excels for communication outside the organization
- Built in key recovery allows perimeter scanning of Mail
- Extremely Scalable

IBE can be a tool to leverage PKI deployments

- Extend the reach of secure communications to people outside the PKI, using a variety of authentication methods
- Provide lightweight encryption for a PKI

For More information about IBE visit
http://www.voltage.com/technology