Identity Based Encryption

Terence Spies

VP Engineering

terence@voltage.com

Voltage Security Overview

- Breakthrough technology for encryption and access control
- Based on work of Dr. Boneh at Stanford and Matt Franklin at UC Davis
  - Unsolved mathematical problem posed by Adi Shamir in 1984
- Company founded in October 2002
- Solving large unmet market demand & opportunity

- Platform play for secure multi-channel communication
  - Voltage SecureMail, SecureFile, SecureIM today
- Toolkit (with source) this spring

Voltage Security Delivers a Unique Solution

- **Anytime and anywhere encryption**
  - No need to expose directories
  - No private key roaming problems
  - Online and offline usage
- **On-demand security**
  - Secure ad hoc communications
- **Easy to use**
  - Transparent to end users
- **Easy to implement**
  - Centralized administration
  - Dynamic group management and access control
  - No rip & replace
- **Strong ROI, low TCO**
  - Ease of deployment, management

What is IBE?

- Next generation public key algorithm
  - Encryption
  - Various novel authentication technologies
- Breaks through barriers associated with prior approaches

"Very few organizations have widely deployed solutions due to concerns over cost, convenience, interoperability, and manageability."

- Ray Wagner, Gartner

How IBE Works

From This Breakthrough…

How Identity Based Encryption Works

The mathematical construct that makes IBE work is a special type of function that is called a Bilinear Map. A Bilinear Map is a pairing that has the special property:

$$Pair(\, \boldsymbol{a} \bullet \boldsymbol{X},\ \boldsymbol{b} \bullet \boldsymbol{Y} \,) = Pair(\, \boldsymbol{b} \bullet \boldsymbol{X},\ \boldsymbol{a} \bullet \boldsymbol{Y} \,)$$

For IBE the operator "•" is multiplication of integers with points on elliptic curves. While multiplication (e.g. calculating $\boldsymbol{a} \bullet \boldsymbol{X}$) is easy, the inverse operation (finding $\boldsymbol{a}$ from $\boldsymbol{X}$ and $\boldsymbol{a} \bullet \boldsymbol{X}$) is practically impossible. The Bilinear Map that is used is a Weil Pairing or Tate Pairing.

To set up the system we pick a secret $\boldsymbol{s}$ and a parameter $\boldsymbol{P}$. Next $\boldsymbol{P}$ and $\boldsymbol{s} \bullet \boldsymbol{P}$ (the product of $\boldsymbol{s}$ and $\boldsymbol{P}$) are distributed to all users. Next we issue to each user their private key. It is the product of their Identity and the secret $\boldsymbol{s}$. For Bob this is $\boldsymbol{s} \bullet \boldsymbol{ID}_{\boldsymbol{Bob}}$.

<u>Sender</u> <u>(Alice)</u>

To encrypt a message to Bob, Alice picks random r and calculates a key k:

$$\boldsymbol{k} = Pair(\, \boldsymbol{r} \bullet \boldsymbol{ID}_{\boldsymbol{Bob}} ,\ \boldsymbol{s} \bullet \boldsymbol{P} \,)$$

We now send to Bob $\mathbf{E}_{\mathbf{k}}$[Message], the message encrypted with k. We also send him the product $\boldsymbol{r} \bullet \boldsymbol{P}$.

E_k[Message]
$\boldsymbol{r} \bullet \boldsymbol{P}$

<u>Receiver</u> <u>(Bob)</u>

After receiving the message, Bob can reconstruct the key $\boldsymbol{k}$ by calculating:

$$\boldsymbol{k} = Pair(\, \boldsymbol{s} \bullet \boldsymbol{ID}_{\boldsymbol{Bob}} ,\ \boldsymbol{r} \bullet \boldsymbol{P} \,)$$

and decrypt the message with it. As Bob is the only person who knows his private key $\boldsymbol{s} \bullet \boldsymbol{ID}_{\boldsymbol{Bob}}$, no one else can calculate $\boldsymbol{k}$.

Voltage security

How IBE Works

… Comes this Elegance

- IBE Public Key:

  info@voltage.com

- RSA Public Key:

Public exponent=0x10001

Modulus=135066410865995223349603216278805969938881
475605667027524485143851526510604859533833940287
150571909441798207282164471551373680419703964191
743046496589274256239341020864383202110372958725
762358509643110564073501508187510676594629205563
685529475213500852879416377328533906109750544334
999811150056977236890927563

Voltage security

BF-IBE

- 1984: IBE suggested by Shamir.
  - No satisfactory solution.

    RSA: cannot map name to pub key = (N,e).

    ElGamal: pub-key = g^x (mod p). PKG cannot get x.

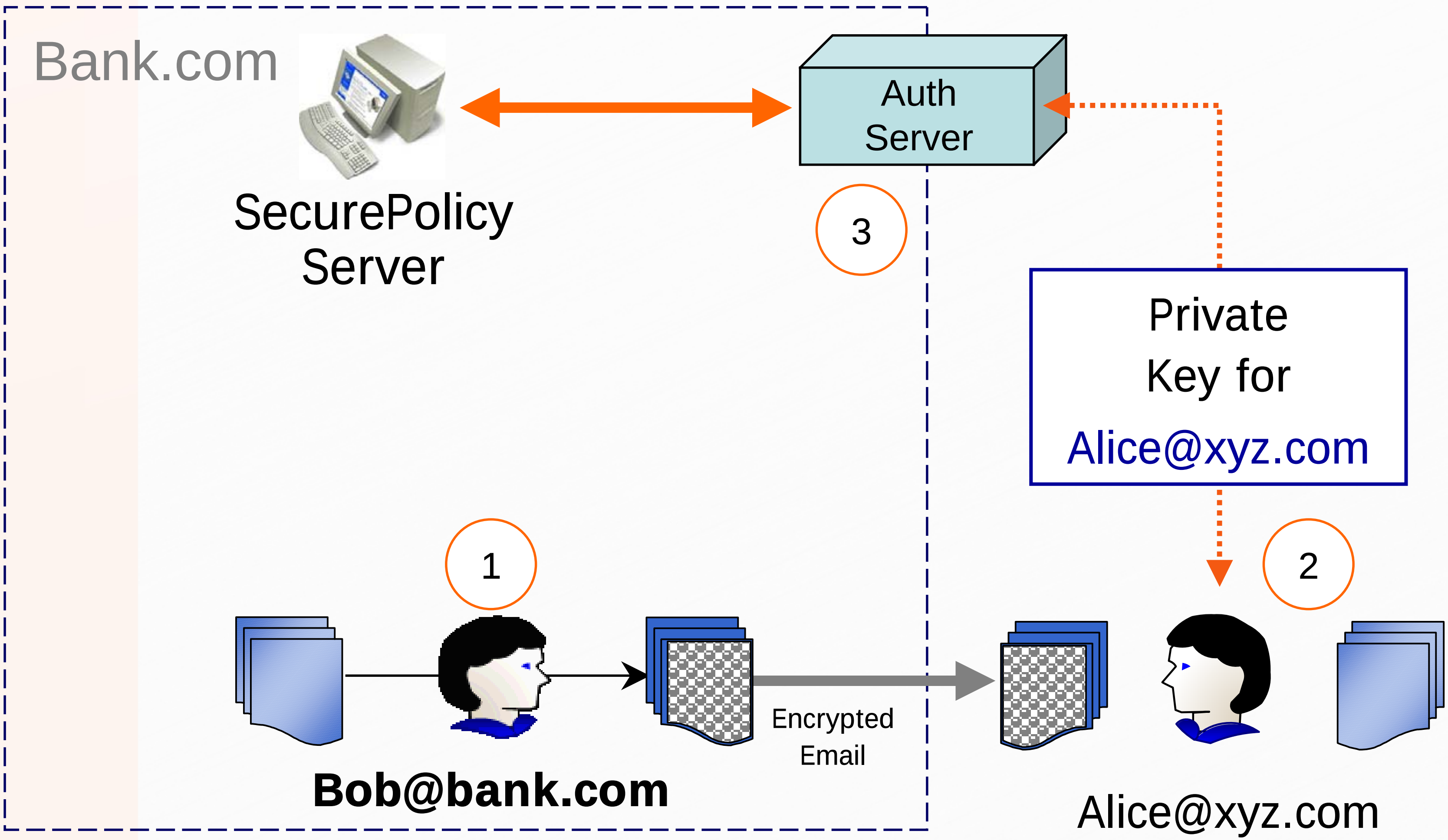
- 2001: Boneh-Franklin (Crypto '01)
  - Practical IBE cryptosystem.
    Based on bilinear maps from algebraic geometry.

- Performance (1024-bit security, 1GhZ P3):
  - Keygen time: 3 ms. CT-size: 160bits+|msg|.
  - Enc/dec time: < 40 ms.

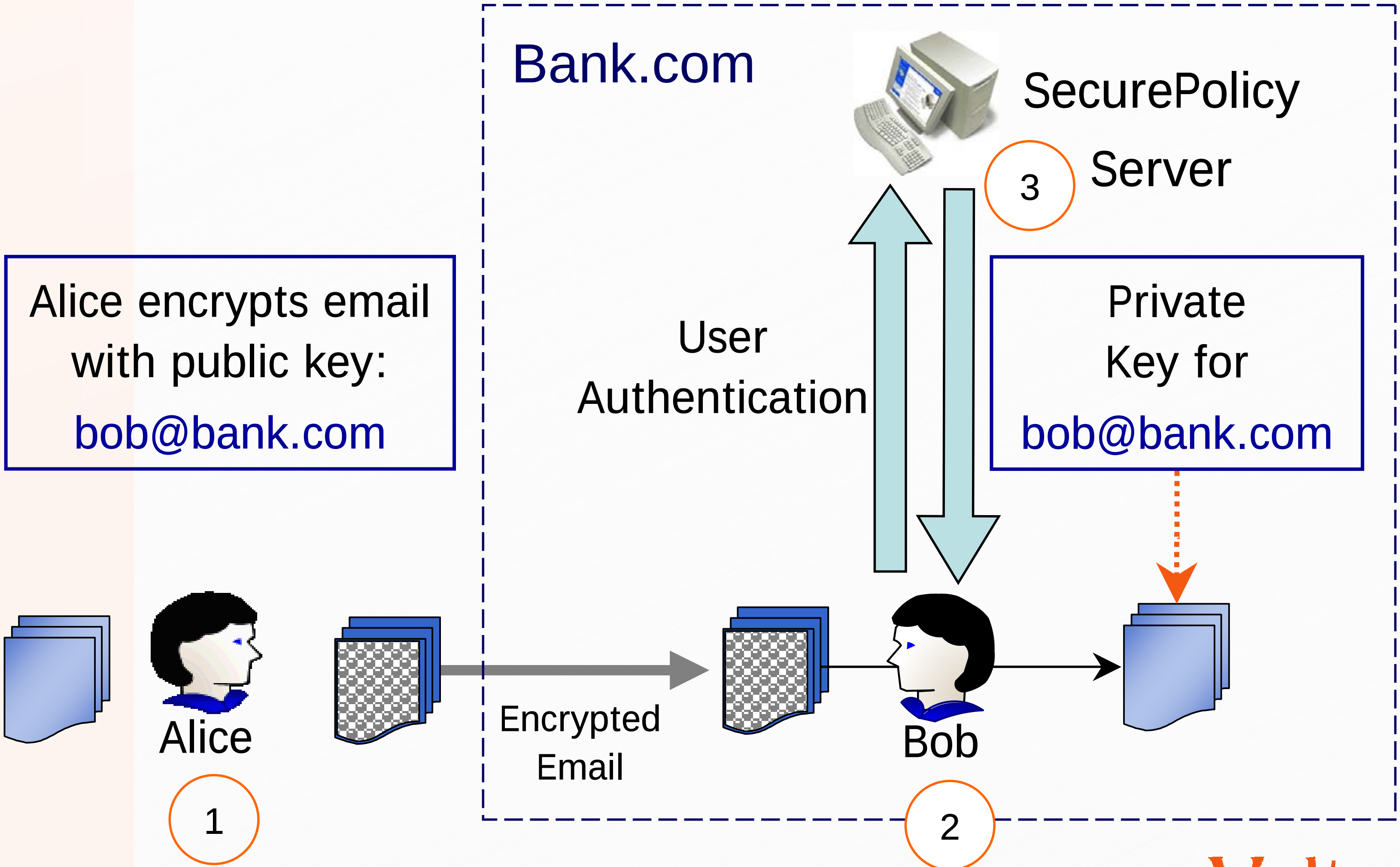
Voltage security

How IBE Works

Power of the system is in its simplicity



How IBE Works
Power of the system is in its simplicity



How IBE Works

- Mapping Identity to Key Server
    - Hub and Spoke – key server is local
    - Partner to Partner – SSL to auth params
    - Will evolve – DNS cert for params
- Administrative Access
    - Customers using gateway for
        - Archive
        - Virus / Spam Scan
        - Mix of gateway and desktop encryption users

Voltage security

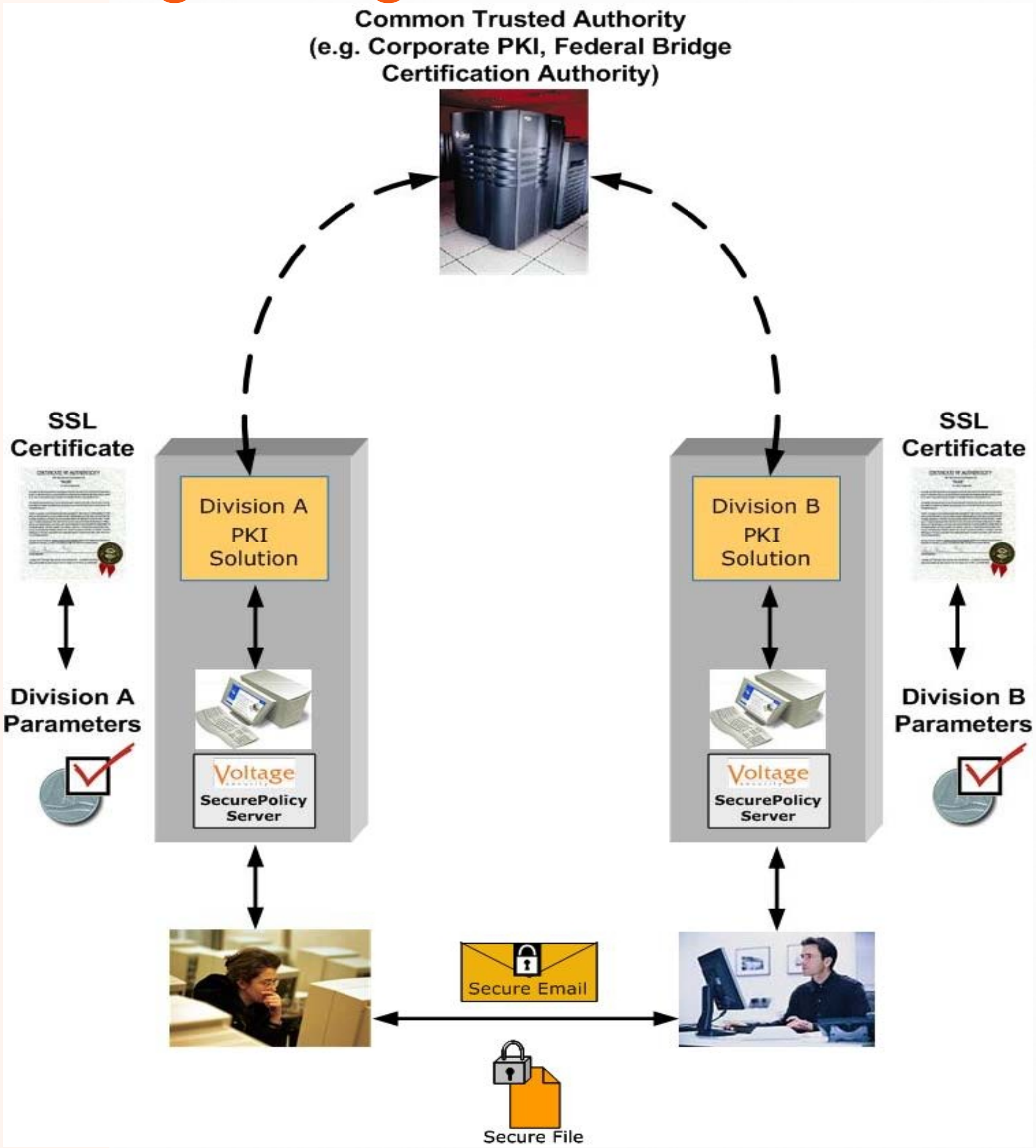
Why are Customers Interested?

- Secure ad-hoc communication for the extended enterprise has become mission critical
  - Multiple channels of communication including messaging, web services
  - People to people, app to people, and app to app
- Government compliance required
  - GLBA, HIPAA
  - FDA 21 CFR Part 11 (Electronic Records and Signatures)
  - Directive 95/46/EC (EU)
  - Sarbanes-Oxley
- Previous products ineffective and expensive to integrate and deploy

Voltage Supports Both Hierarchical and Federated Trust Models

- Voltage Policy Server chains to traditional PKI and supports PKI for signature
- Hub & spoke deployment allows for robust know-your-customer policies & central authentication
- Federated deployment allows for trusted peer organizations to perform authentication of local district users

Voltage Integrates with an Existing PKI



IBE + PKI Benefits

Payback on PKI investment while gaining easier to use and deploy system

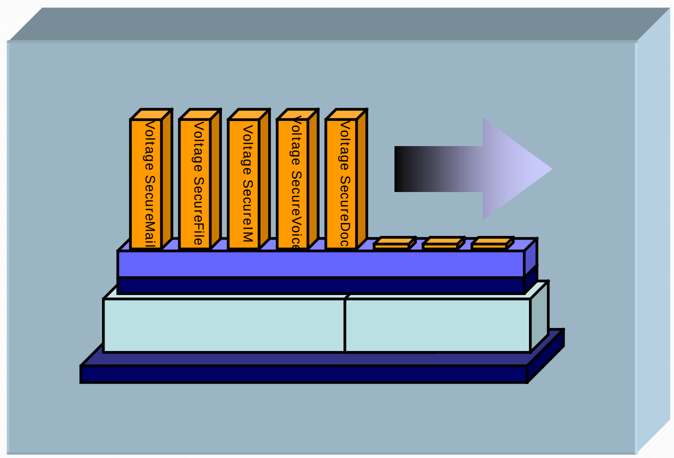
Communication between trusted domains

Lower cost rollout of secure system across enterprise

Voltage Security Platform Fits Into Your Current Architecture

Integrates to your current Application(s) – Messaging, IM, Documents, VoIP

Enterprise Messaging



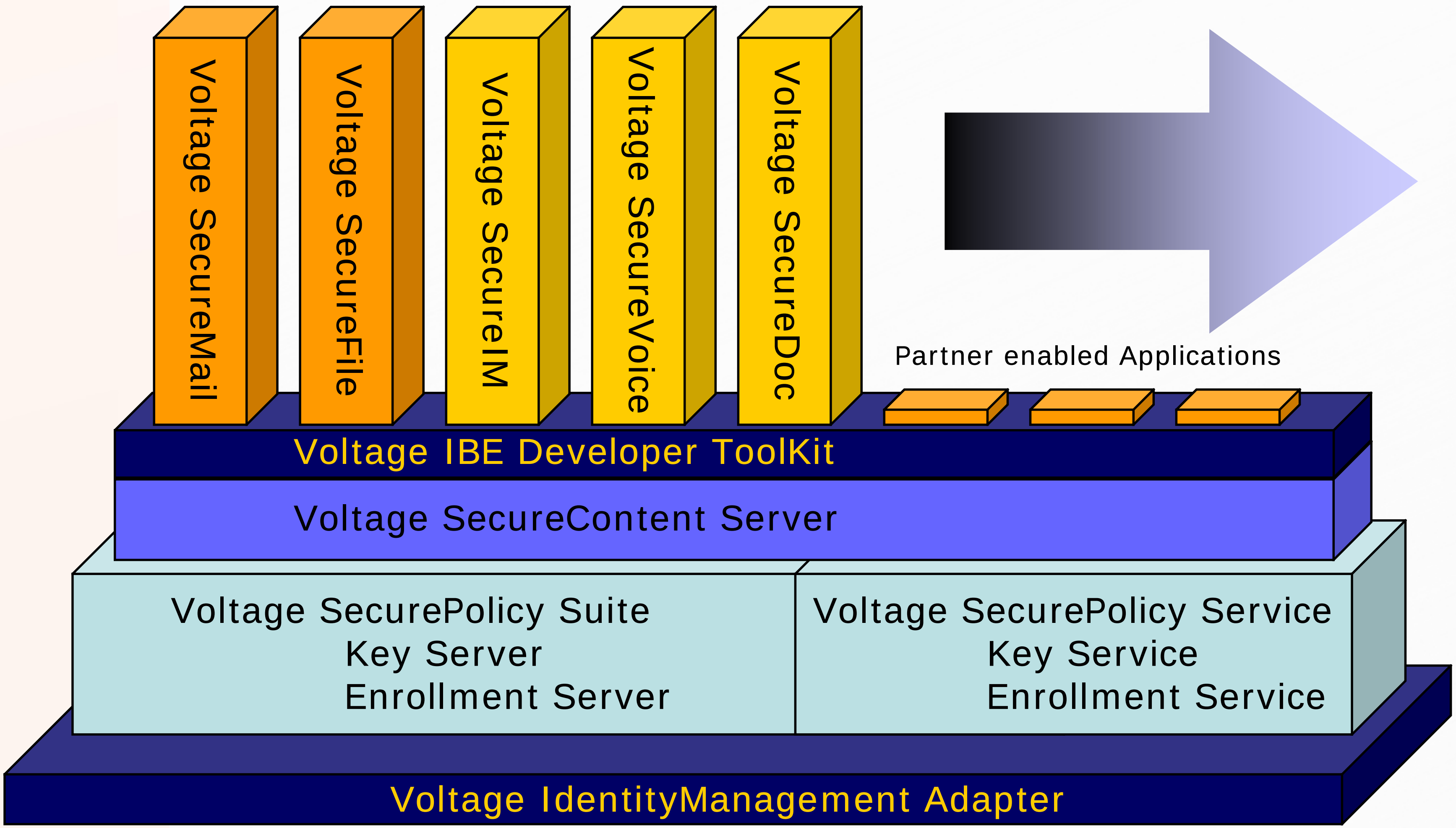
Enterprise LDAP Directory

Tap Into Current Identity Structure

Data at Rest

Secure business critical data accessed via portals or applications

The Voltage Security Platform



Voltage security

Importance of Email

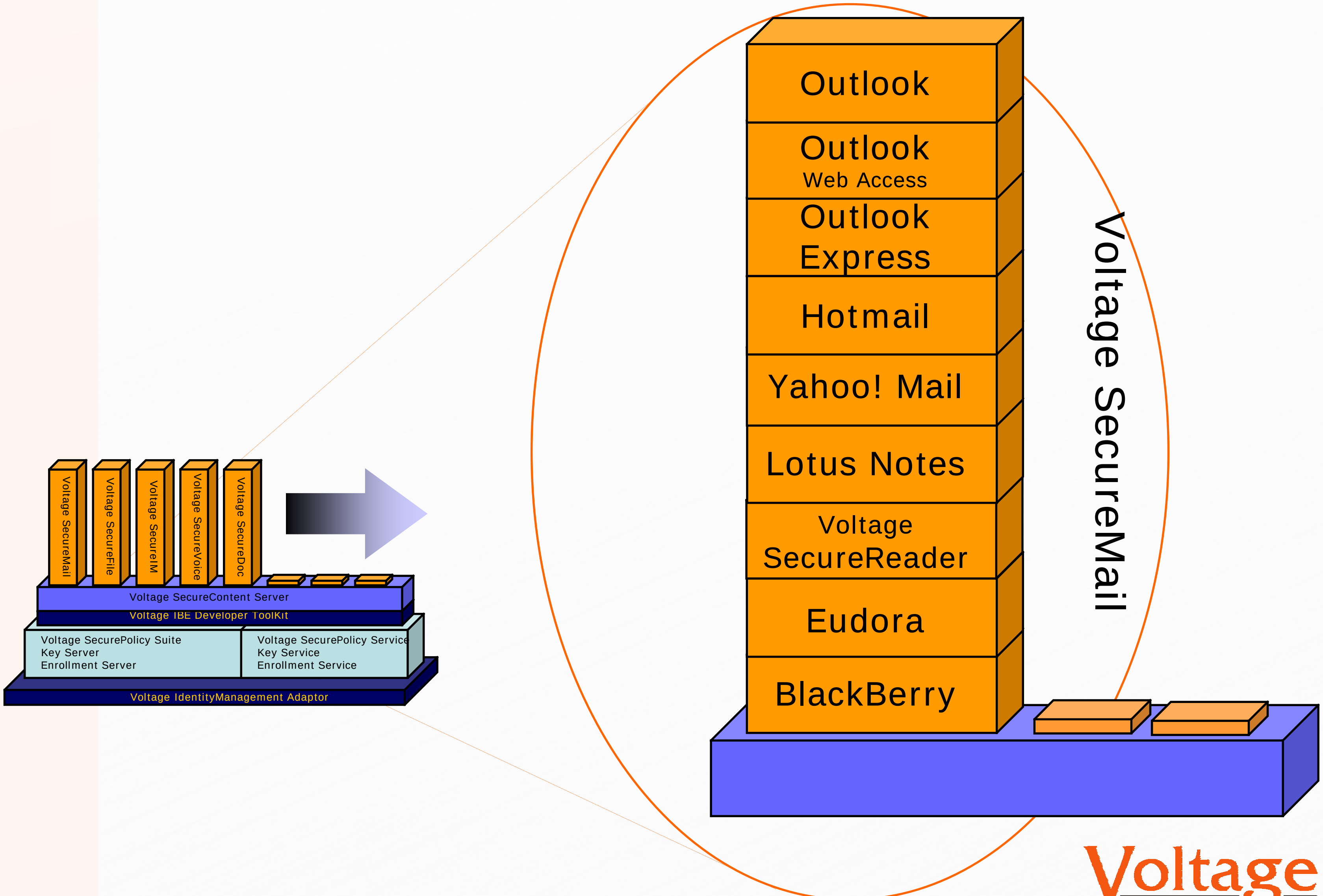
Gartner estimates that 75% of the total knowledge exchange occurring via email contains proprietary intellectual property and must be protected as a valuable corporate asset.

3 out of 4 emails should be protected as valuable corporate assets

Source: Gartner

Voltage security

The Voltage SecureMail™ Solution



Zero Footprint Support
Achieving 100% client support with no downloads!

- Set of configurations for ensuring comprehensive coverage of end-user environments
- For Consumer oriented Applications
  - Zero Footprint Reader – browser based
- For Enterprise applications
  - Voltage SecureGateway

Voltage security

Plugin compared to Browser access

Voltage supports both models

Desktop plug-ins

Pros:
Native user agent
Transparent to end user

Cons:
One-time software download
Ongoing maint. & help desk

Browser access

Pros:
100% coverage

Cons:
Browser user agent
Means changing end user behavior

Voltage Security architecture

Tight Integration
With Desktop

Zero Footprint
On Desktop

Summary

- Breakthrough technology for secure anytime, anywhere communications
- Based on work of Dr. Boneh at Stanford and Matt Franklin at UC Davis
  - Unsolved mathematical problem posed by Adi Shamir in 1984
- Solving large unmet market demand opportunity

- Platform play
  - Voltage SecureMail, SecureFile, SecureIM today
  - SecureDoc, SecureVPN… all forthcoming

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.

Voltage security